SLI-5460 / SLI-5460-I

Benutzerhandbuch

ADSL IAD – Satellit optimiert

Release V1.04 | 2010-03

Internetagentur Schott GmbH
Cent-Hoheneichstr. 11
D-96191 Trunstadt

© Internetagentur Schott GmbH., 2010. All rights reserved.

Deutschland
Alle Elektro- und Elektronikgeräte sind getrennt vom allgemeinen Hausmüll über dafür staatlich vorgesehene Stellen zu entsorgen.

Wenn dieses Symbol eines durchgestrichenen Abfalleimers auf einem Produkt angebracht ist, unterliegt dieses Produkt der europäischen Richtlinie 2002/96/EC.

Die getrennt Sammlung von Altgeräten und deren sachgemäße Entsorgung dienen der Vorbeugung von potenziellen Umwelt- und Gesundheitsschäden. Sie sind eine Voraussetzung für die Wiederverwertung und das Recycling gebrauchter Elektro- und Elektronikgeräte.

Ausführlichere Informationen zur Entsorgung Ihrer Altgeräte erhalten Sie bei Ihrer Kommune, Ihrem Müllentsorgungsdienst oder dem Fachhändler, bei dem Sie das Produkt erworben haben.

Schweiz
Dieses Produkt darf am Ende seiner Lebensdauer nicht über den normalen Haushaltabfall entsorgt werden, sondern muss einer Verkaufsstelle oder einem Sammelpunkt für das Recycling von elektrischen und elektronischen Geräten abgegeben werden gemäss Verordnung über Rückgabe, Rücknahme und Entsorgung elektrischer und elektronischer Geräte (VREG).

Die Werkstoffe sind gemäss ihrer Kennzeichnung wieder verwertbar. Mit der Wiederverwendung, der stofflichen Verwertung oder anderer Formen der Verwertung von Altgeräten leisten Sie einen wichtigen Beitrag zum Schutze der Umwelt.

Sicherheitsbestimmungen

- Platzieren Sie das Gerät in der Nähe einer Steckdose.
- Benutzen Sie ausschliesslich das mitgelieferte Steckernetzteil und verwenden Sie dieses nicht für andere Geräte.
- Alle Kabel, welche an die mit Ethernet 1-4; 1 und 2 bezeichneten Schnittstellen angeschlossen werden, müssen **innerhalb** eines Gebäudes bleiben. Verwenden Sie dieses Gerät und das Zubehör nur in Innenräumen.
- Schützen Sie das Gerät vor direkter Sonneneinstrahlung, Wasser und anderen Flüssigkeiten sowie starkem Staub. Betreiben Sie das Gerät nur in trockenen Räumen; der Betrieb in feuchten (z.B. Badezimmer) oder explosionsgefährdeten Räumen ist verboten.
- Reinigen Sie das Gerät mit einem weichen, trockenen Tuch. Tauchen Sie das Gerät niemals in Wasser oder andere Flüssigkeiten ein.
- Öffnen oder reparieren Sie niemals das Gerät oder das Steckernetzteil.
- Das Gerät kann medizinische Geräte in ihrer Funktion beeinträchtigen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Inhaltsverzeichnis

1. Einleitung 5
1.1. Zweck und Umfang dieses Dokumentes 5
1.2. Merkmale 5
1.3. Einige Erklärungen zur Bedienungsanleitung 6
2. Anzeigen, Anschlüsse und Bedienelemente 7
2.1. Vorderseite 7
2.1.1. Besonderer Zustand 8
2.2. Rückseite 9
3. Anschliessen des IADs 10
3.1. PC System Voraussetzungen 10
3.2. Konfigurieren des PCs (TCP / IP Einstellungen) 10
3.2.1. Windows 2000 11
3.2.2. Windows XP 13
3.2.3. Windows Vista 15
3.2.4. MAC OS 9.x 16
3.2.5. MAC OS X 17
3.3. Anschliessen des ADSL Kabels, Computers und Stechernetzteils 19
3.3.1. LAN Verbindung 19
3.3.2. Telefonverbindung 19
3.3.3. Anschliessen des ADSL- und Festnetzkabels 20
3.3.4. Stromanschluss 21
3.4. Überprüfen der LEDs 21
4. Aufrufen des Schnellstarts 22
5. Konfiguration 24
5.1. Status 25
5.1.1. Geräteinformation 25
5.1.2. VOIP Status 25
5.1.3. ADSL-Anschluss 26
5.1.4. Internet Verbindung 27
5.1.5. Traffic Statistik 27
5.1.6. DHCP-Tabelle 28
5.1.7. WLAN Clients 29
5.1.8. Routing Tabelle (Experten) 30
5.1.9. NAT Tabelle (Experten) 31
5.1.10. ARP-Tabelle 31
5.2. Schnellstart 32
5.3. Erweitert 37
5.3.1. Lokales Netzwerk 37
5.3.2. Internet (Experten) 42
5.3.3. IP Routing (Experten) 51
5.3.4. Virtuelle Server 52
5.3.5. NAT ALG (Experten) 58
5.3.6. Firewall (Experten) 59
5.3.7. Jugendschutz 67
5.3.8. QoS 70
5.3.9. Portzuordnung (Experten) 73
5.4. Wireless 74
5.4.1. Grundeinstellungen 74
5.4.2. Sicherheit 75
5.4.3. Zugangskontrolle 80
5.4.4. Signalverstärker (Repeater) 81
5.5. VOIP 83
5.5.1. SIP Einstellungen (Experten) 83

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.5.2. SIP Konten 86
5.5.3. Anschlusseinstellungen 87
5.5.4. PSTN Wählplan (Experten) 89
5.5.5. VOIP Wählplan (Experten) 92
5.5.6. Anrufeinstellungen 94
5.5.7. Schnellwahl 95
5.5.8. Klingeln & Töne (Experten) 95
5.6. Management 96
5.6.1. Management Konten 96
5.6.2. Management Kontrolle (Experten) 98
5.6.3. Diagnose 99
5.6.4. Email Benachrichtigung (Experten) 100
5.6.5. TR-069 Client (Experten) 100
5.6.6. SNMP Agent (Experten) 101
5.6.7. Internetzeit 103
5.6.8. Zeitplan 104
5.6.9. System Log (Experten) 106
5.6.10. Backup Konfiguration 106
5.6.11. Firmware Upgrade 107
5.6.12. Neustart 108
5.7. Konfiguration speichern 108
5.8. Abmelden 108
6. Anhang 109
6.1. Werkseinstellungen 109
6.2. Zugriff auf die Weboberfläche 109
6.3. Anleitung für Zusatzdienste 109
7. Fehlerbehebung 110
8. SAT - Optimierung 110-111
9. Copyright und Lizenzen 112
9.1. GNU GPL – General Public License 112
10. Glossar 113
10.1. Tabelle mit Abkürzungen 120
11. CE-Konformitätserklärung 122

© Internetagentur Schott GmbH, 2010. All rights reserved.

1. Einleitung

1.1. Zweck und Umfang dieses Dokumentes

Dieses Dokument gibt Ihnen Schritt für Schritt Anweisungen zur Installation / Betrieb des Gerätes und bietet zusätzliche technische Informationen. Dieses Dokument wird von Internetagentur Schott GmbH zur Verfügung gestellt. Es kann von einem Provider als Vorlage genutzt werden. Die netzwerkspezifischen Konfigurationsdaten mit der grafischen Benutzeroberfläche (GUI) hängen von ihrem ISP ab.
Bitte befolgen Sie die in diesem Benutzerhandbuch zu findenden Anweisungen sorgfältig. Bewaren Sie dieses Benutzerhandbuch in der Nähe Ihres Gerätes auf und schauen Sie darin nach, wenn etwas nicht funktioniert. Schäden, die aus unsachgemässer Handhabung resultieren, führen zum Garantieverlust.

1.2. Merkmale

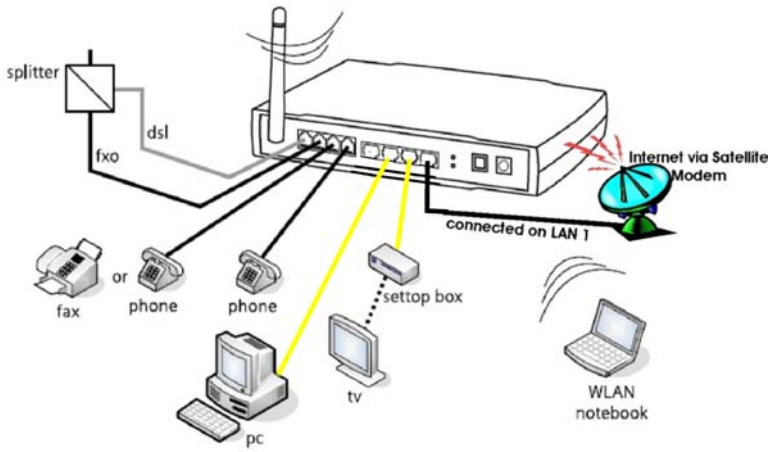
Das IAD SLI-5460 ist ein ADSL/ Internet via Satellit Breitbandzugriffs-Gateway speziell entwickelt für den Tripple-play-Einsatz: High Speed Internet, IPTV, sowie Video on Demand und VoIP-Telefonie über eine einzige Breitband Verbindung.

Umfangreiche Servicequalitätsmechanismen (QoS) helfen hohe Servicequalitäten im Bereich VoIP und IPTV sicherzustellen. Das SLI-5460 beinhaltet ein ADSL2+ Modem (wird bei Internet via Satellit Betrieb nicht benötigt), Router, Firewall, Wireless b/g Access Point, 4 Port Ethernet Switch (bei SAT-Betrieb 3 Port) und 2 VoIP Ports in einem Gerät.

Bestehende Analogtelefone und Faxe können mit dem IAD SLI-5460 verbunden werden. Anrufe können entweder über das Internet oder alternativ dazu über das Festnetz getätigt werden.

Dieses IAD ist sehr einfach zu installieren / konfigurieren und kombiniert den bestehenden Internetservice mit den neuen Services IP-TV und Voice over IP in einem einzigen Gerät.

Typische Anwendung



© Internetagentur Schott GmbH, 2010. All rights reserved.

1.3. Einige Erklärungen zur Bedienungsanleitung

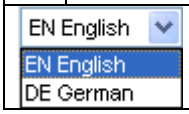
Um diese Anleitung so klar wie möglich zu halten, bitten wir Sie, die folgende Seite zu lesen. Sie erklärt die Bedeutung häufig benutzter Symbole.

	Checkbox
☑	Dieses Symbol zeigt eine aktive Checkbox; die beschriebene Funktion ist aktiviert.
☐	Dieses Symbol zeigt eine inaktive Checkbox; die beschriebene Funktion ist deaktiviert.

Checkboxen erlauben eine Mehrfachauswahl und werden normalerweise bei entsprechenden Funktionen eingesetzt, welche nicht zwingend gebraucht werden.

	Radio Buttons
◉	Dieses Symbol zeigt einen aktiven Radio Button; Wenn dieser Button-Typ eingesetzt wird, muss eine Auswahl erfolgen, damit fortgefahren werden kann.
○	Dieses Symbol zeigt einen inaktiven Radio Button

Radio Buttons geben eine Auswahl zwingender Funktionen. Man muss einen selektieren und es ist nicht möglich mehr als einen auszuwählen.

	Pull-Down Menü (Liste)
	Ein Pull-Down Menü beinhaltet eine Liste, aus der Sie eine Option auswählen können. Die Liste sehen Sie, in dem Sie auf das kleine blaue Dreieck drücken.

Ein Pull-Down Menü zeigt eine Auswahl grafisch anders an als Radio Buttons, funktioniert im Prinzip aber gleich.

Einige Seiten sind nur empfohlen für fortgeschrittene Benutzer. Diese Seiten sind nur verfügbar, wenn man sich im Gerät als admin einloggt. Diese Seiten sind entsprechend gekennzeichnet (mit „Experten“).

Es gibt Seiten, welche durch mehrere Menü-Einträge zu erreichen sind. In jedem Menü-Eintrag werden nur die relevanten (grün markiert) Teile erklärt.

In dieser Anleitung wird die Bezeichnung „Gerät“ für das SLI-5460 / SLI-5460-I verwendet.

© Internetagentur Schott GmbH, 2010. All rights reserved.

2. Anzeigen, Anschlüsse und Bedienelemente

2.1. Vorderseite

LED		Bedeutung
1	Power	Ist aus, wenn das Gerät keinen Strom hat.
		Leuchtet grün, wenn das Gerät mit Strom versorgt wird.
		Leuchtet orange, wenn ein Systemfehler vorliegt.
2	Ethernet 1 - 4	Ist aus, wenn kein Computer in der entsprechenden Buchse mit dem Gerät verbunden ist.
		Leuchtet grün oder orange, wenn ein Computer in der entsprechenden Buchse mit dem Gerät verbunden ist.
		Leuchtet grün, wenn eine Verbindung mit 100Mbps steht.
		Leuchtet orange, wenn eine Verbindung mit 10Mbps steht.
		Blinkt grün oder orange während eines Datentransfers.
3	Wireless	Ist aus, wenn der Wireless Access Point deaktiviert ist.
		Leuchtet grün bei aktivem Wireless Access Point.
		Blinkt grün während eines Datentransfers.
		Blinkt langsam grün, wenn neue WPS-Clients sich mit dem WLAN verbinden dürfen.
4	1, 2 *	Ist aus, wenn das entsprechende Telefon aufgelegt ist.

* Diese LEDs wechseln Ihren Status nur, wenn VoIP konfiguriert ist.

© Internetagentur Schott GmbH, 2010. All rights reserved.

		Leuchtet grün, wenn das entsprechende Telefon abgenommen wird.
		Blinkt grün, wenn das Festnetz anstatt Internettelefonie (VoIP) benutzt wird.

LED		Bedeutung
5	Line*	Ist aus, wenn das Festnetz (PSTN) nicht benutzt wird.
		Leuchtet grün, wenn das Festnetz benutzt wird.
6	VoIP*	Ist aus, wenn die Internettelefonie ausgeschaltet ist.
		Leuchtet, wenn die SIP Registration erfolgreich war. Grün für das Telefon 1; orange für das Telefon 2
		Bemerkung: Die VoIP LED leuchtet ebenfalls orange, wenn die Registration beider Linien erfolgreich war.
7	DSL	Ist aus, wenn das Gerät so konfiguriert ist, dass es nicht ADSL nutzt, um eine Verbindung mit dem Internet herzustellen.
		Leuchtet grün, wenn eine ADSL Verbindung aufgebaut ist („line sync").
		Blinkt langsam grün, wenn es nach einem ADSL Signal sucht.
		Blinkt schnell grün während es eine ADSL Verbindung aufbaut („line is synchronizing").
8	Internet	Ist aus, wenn sicht das Gerät im „Bridged Mode" befindet, oder keine WAN Verbindung vorhanden ist.
		Leuchtet grün, wenn eine Internetverbindung via Satelliten Modem erfolgreich aufgebaut wurde.
		Blinkt grün während eines Datentransfers.

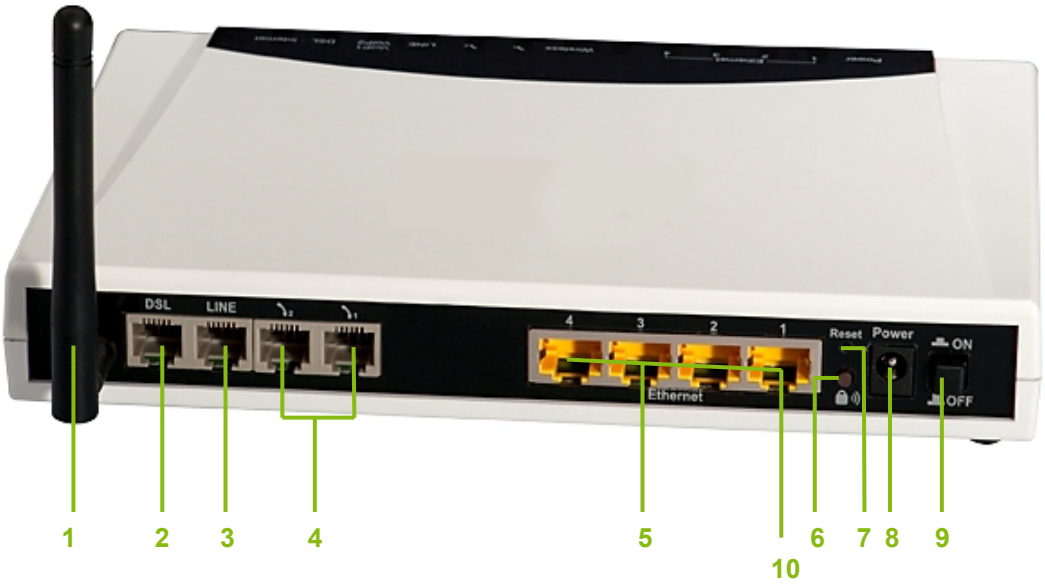
2.1.1. Besonderer Zustand

Wenn die Power LED orange leuchtet und die ADSL sowie Internet LED gleichzeitig blinken, dann wird das Gerät auf die Werkseinstellungen zurückgesetzt. Dieser Zustand erscheint, wenn Sie den Reset Button für mindestens 5 Sekunden gedrückt halten. Danach müssen Sie den Stromschalter einmal aus- und wieder einschalten. Erst dann wird das Gerät auf die Werkseinstellungen zurückgesetzt.

* Diese LEDs wechseln Ihren Status nur, wenn VoIP konfiguriert ist.

© Internetagentur Schott GmbH, 2010. All rights reserved.

2.2. Rückseite



Buchse		Bedeutung
1	Antenne	Schrauben Sie hier die mitgelieferte Antenne an.
2	DSL	Verbinden Sie das graue ADSL Kabel mit dieser Buchse.
3	Line	Verbinden Sie das schwarze PSTN Kabel mit dieser Buchse.
4	☎_2	Verbinden Sie das Telefon 2 mit dieser Buchse.
	☎_1	Verbinden Sie das Telefon 1 mit dieser Buchse.
5	Ethernet	Verbinden Sie Ihre Computer mit diesen Buchsen.
6	WPS / WLAN	Drücken Sie den Knopf weniger als 5 Sekunden, um WLAN Clients, die WPS benützen, hinzuzufügen.
		Drücken Sie den Knopf länger als 5 Sekunden, um das WLAN zu aktivieren / deaktivieren.
7	Reset	Drücken Sie den Knopf weniger als 5 Sekunden, um das Gerät neu zu starten.
		Drücken Sie den Knopf länger als 5 Sekunden, um das Gerät auf die Werkseinstellungen zurückzusetzen. (Alle LEDs leuchten auf). Danach müssen Sie das Gerät mit Hilfe des Stromschalters aus-/einschalten, um die Änderungen wirksam zu machen.
8	Strom	Verbinden Sie das mitgelieferte Netzteil.
9	Stromschalter	Drücken Sie den Stromschalter, um das Gerät ein- / auszuschalten.
10	Ethernet WAN **LAN 1**	Schließen Sie hier Ihr Internet via Satellit Modem an

© Internetagentur Schott GmbH, 2010. All rights reserved.

3. Anschliessen des IADs

Die farbigen Buchsen und Kabel machen das Anschliessen besonders einfach; verbinden Sie die farbigen Kabel jeweils mit der farblich korrespondierenden Buchse am IAD. **(Bei Satellit verbinden Sie LAN 1 mit dem Satellitenmodem per Netwerkkabel)**

3.1. PC System Voraussetzungen

Bevor Sie mit der Installation des IADs beginnen, stellen Sie sicher, dass:

- Ihr Computer mit einer LAN-Schnittstelle mit RJ-45 ausgerüstet ist.
- Sie einen Internet-Browser (z.B. Internet Explorer oder Firefox) installiert haben.

3.2. Konfigurieren des PCs (TCP / IP Einstellungen)

Die Konfiguration Ihres PCs ist abhängig vom installierten Betriebssystem. Die folgenden Betriebssysteme werden durch die vorliegende Kurzanleitung abgedeckt:

Windows 2000	MAC OS 9.x
Windows XP	MAC OS X
Windows Vista	

Fahren Sie nun mit jenem Abschnitt fort, welcher das auf Ihrem PC installierte Betriebssystem zum Inhalt hat.

© Internetagentur Schott GmbH, 2010. All rights reserved.

3.2.1. Windows 2000

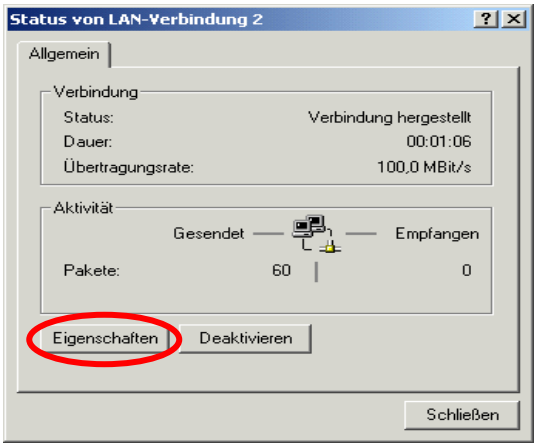
1. Klicken Sie auf ***Start*** → ***Einstellungen*** → ***Systemsteuerung.***

   Doppelklicken Sie das Symbol ***Netzwerk- und DFÜ-Verbindungen.***

   Nun erscheint das Fenster ***Netzwerk*** (ohne Abbildung).

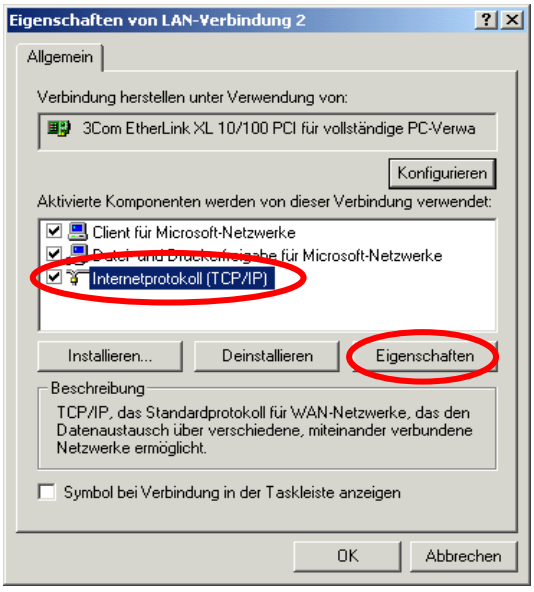
2. Doppelklicken Sie das Symbol ***LAN-Verbindung*** der verwendeten Netzwerkkarte (oft an erster Stelle aufgeführt).

   Klicken Sie auf ***Eigenschaften.***



3. Markieren Sie die Zeile ***Internet Protokoll (TCP/IP).***

   Klicken Sie auf ***Eigenschaften.***

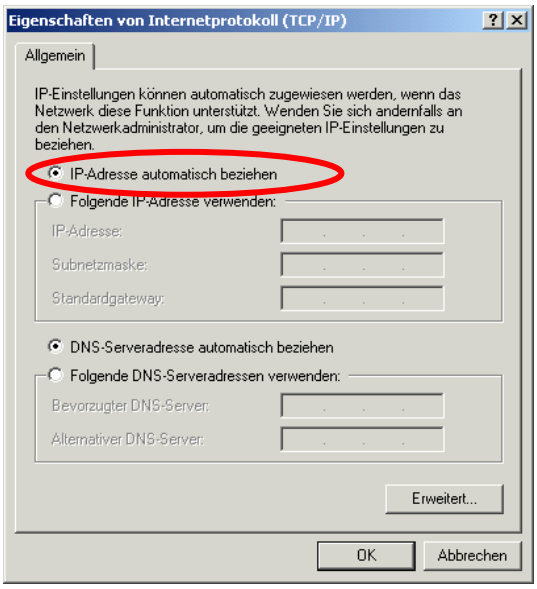


© Internetagentur Schott GmbH, 2010. All rights reserved.

4. Selektieren Sie ***IP-Adresse automatisch beziehen.***

   Klicken Sie ***OK,*** um die PC-Konfiguration abzuschließen.

5. Starten Sie Ihren PC neu.



© Internetagentur Schott GmbH, 2010. All rights reserved.

3.2.2. Windows XP

Die folgenden Anweisungen beruhen auf der Annahme, dass Sie die Windows XP Standardoberfläche verwenden. Falls Sie die klassische Oberfläche verwenden (Menus und Symbole sehen gleich aus wie bei früheren Windows Versionen), folgen Sie bitte den Anweisungen für Windows 2000.

1. Klicken Sie auf ***Start → Systemsteuerung.***

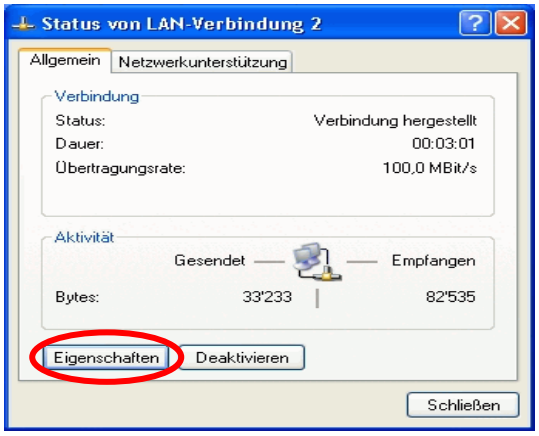
   Klicken Sie auf das Symbol ***Netzwerk- und Internetverbindungen.***

   Klicken Sie auf das Symbol ***Netzwerkverbindungen.***

   Nun erscheint das Fenster ***Netzwerk*** (ohne Abbildung).

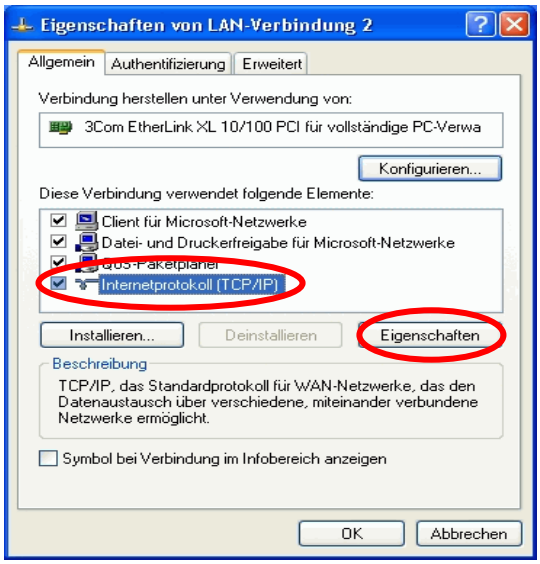
2. Doppelklicken Sie das Symbol ***LAN-Verbindung*** der verwendeten Netzwerkkarte (oft an erster Stelle aufgeführt).

   Klicken Sie nun auf ***Eigenschaften.***



3. Markieren Sie die Zeile ***Internet Protokoll (TCP/IP).***

   Klicken Sie auf ***Eigenschaften.***

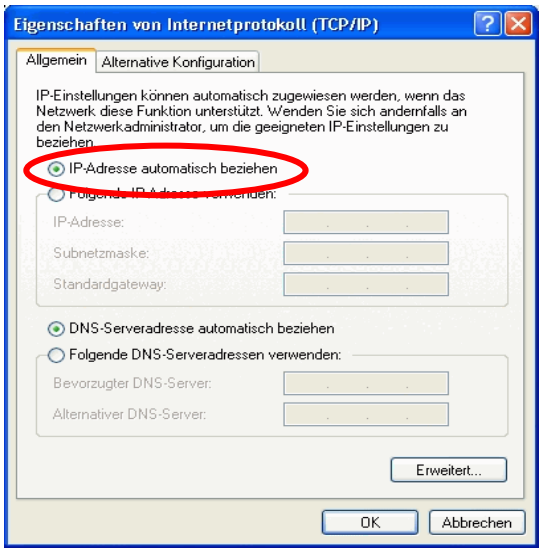


© Internetagentur Schott GmbH, 2010. All rights reserved.

4. Selektieren Sie ***IP-Adresse automatisch beziehen.***

   Klicken Sie ***OK,*** um die PC-Konfiguration abzuschließen.

Starten Sie Ihren PC neu.



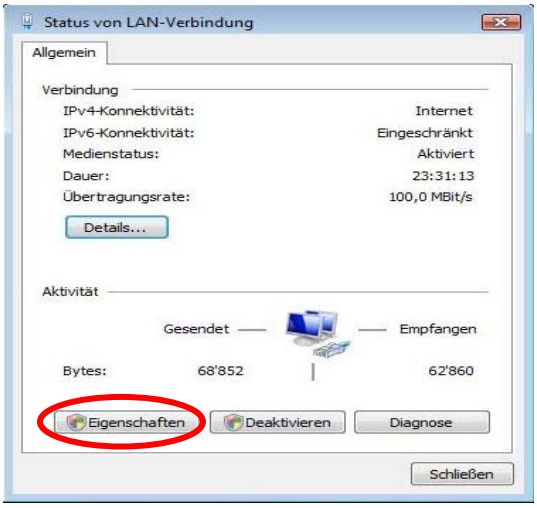
© Internetagentur Schott GmbH, 2010. All rights reserved.

3.2.3. Windows Vista

1. Klicken Sie auf ***Start → Systemsteuerung.***

   Klicken Sie auf das Symbol ***Netzwerk- und Freigabecenter.***

   Klicken Sie auf ***LAN-Verbindung → Status anzeigen.***

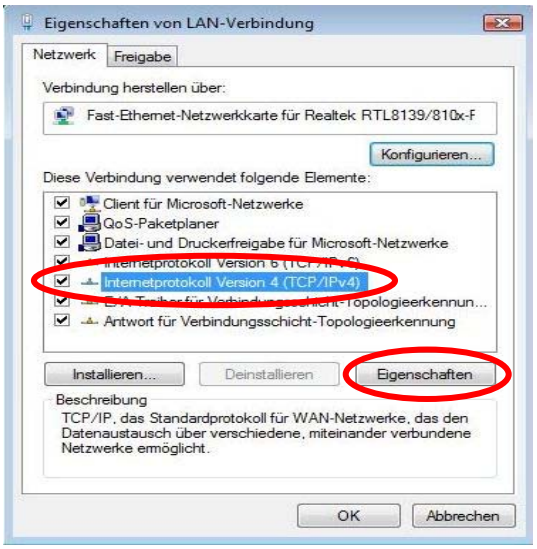


2. Nun erscheint das Fenster ***Status von LAN-Verbindungen***.

   Klicken Sie auf ***Eigenschaften.***

3. Markieren Sie ***Internet Protokoll Version 4 (TCP/IPv4).***

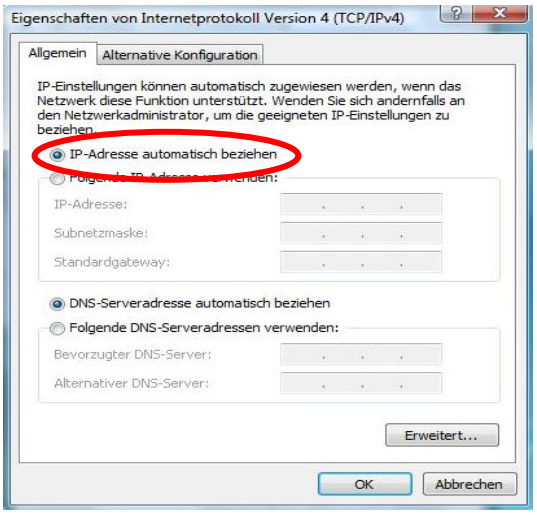
   Klicken Sie auf ***Eigenschaften.***



4. Selektieren Sie ***IP-Adresse automatisch beziehen.***

   Klicken Sie ***OK,*** um die PC-Konfiguration abzuschließen.

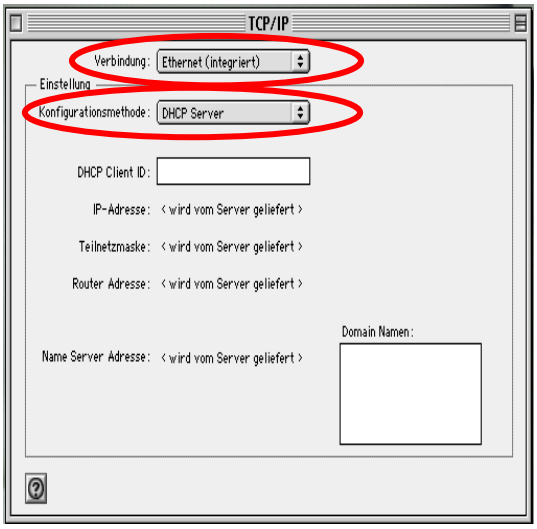
Klicken Sie ***OK,*** um die Konfiguration abzuschließen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

3.2.4. MAC OS 9.x

1. Wählen Sie im ***Apfel-Menü Kontrollfelder → TCP/IP.***



2. Aus dem Pull-Down Menü *Verbindung* wählen Sie ***Ethernet (integriert).***

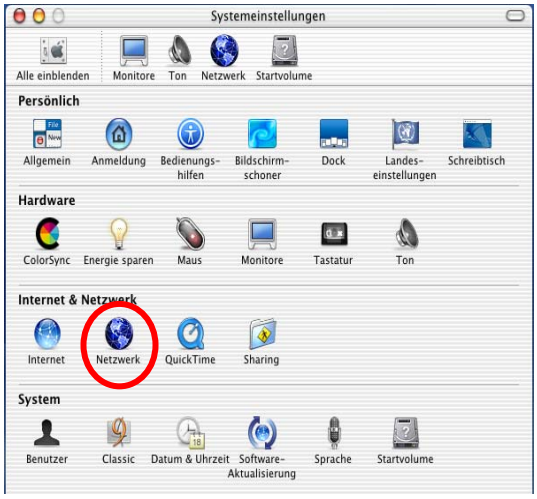
   Aus dem Pull-Down Menü *Konfigurationsmethode* wählen Sie ***DHCP Server.***

3. Schließen Sie das ***TPC/IP-Fenster*** und klicken Sie auf ***speichern.***

© Internetagentur Schott GmbH, 2010. All rights reserved.

3.2.5. MAC OS X

1. Wählen Sie im ***Apfel-Menü Systemeinstellungen.***

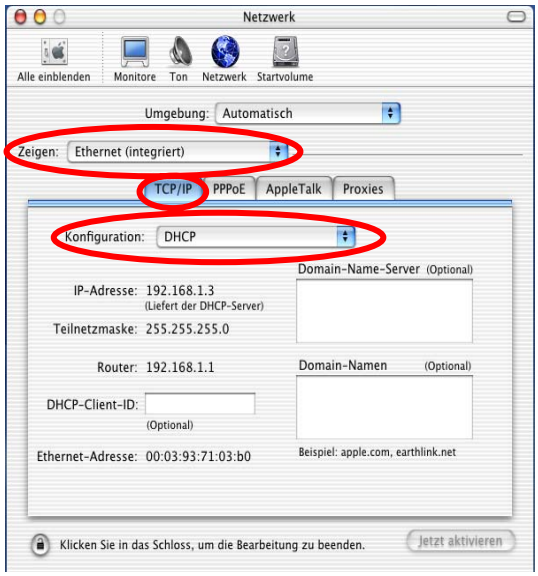


2. Klicken Sie im Bereich *Internet & Netzwerk* auf das Symbol ***Netzwerk.***

3. Aus dem Pull-Down Menü ***Zeigen*** wählen Sie ***Ethernet (integriert).***

   Klicken Sie das Register ***TCP/IP*** an.

   Im Pull-Down Menü ***Konfiguration*** wählen Sie ***DHCP.***



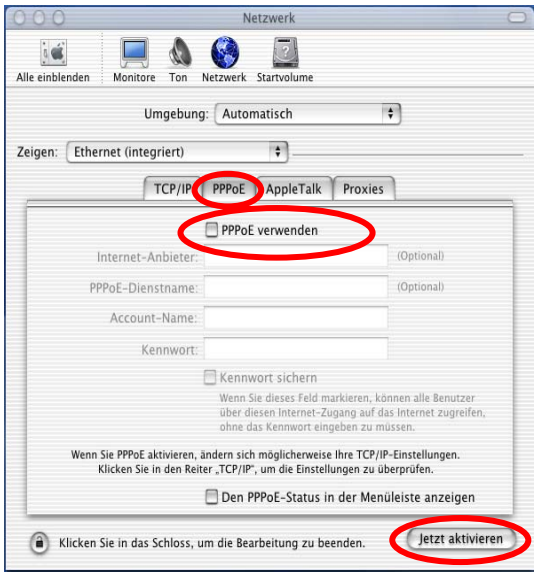
© Internetagentur Schott GmbH, 2010. All rights reserved.

4. Wählen Sie nun das Register ***PPPoE*** an.

   Vergewissern Sie sich, dass die Checkbox ***PPPoE verwenden*** nicht aktiviert ist.

   Klicken Sie auf ***jetzt aktivieren.***

5. Schließen Sie das Fenster ***Netzwerk.***

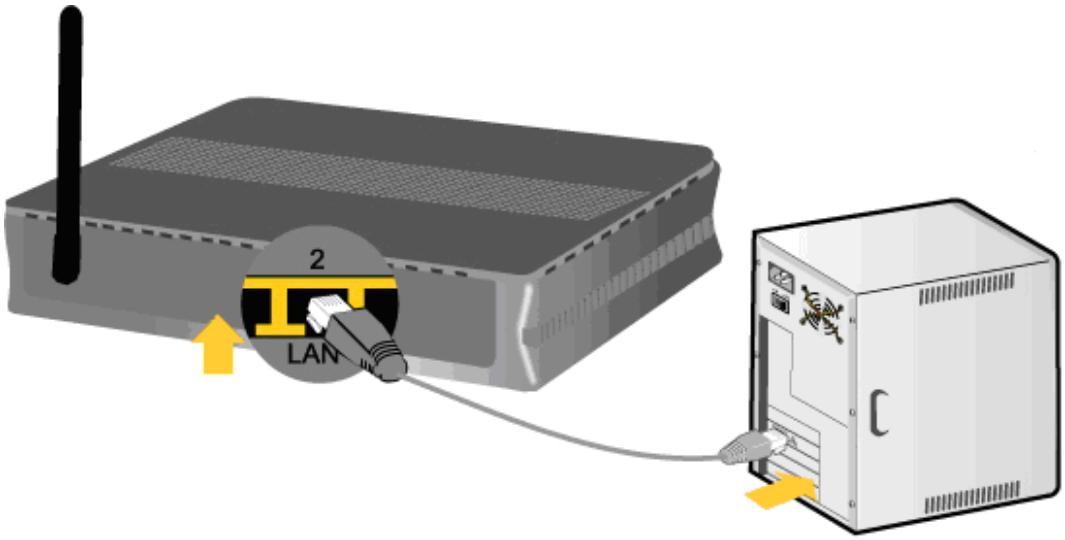


© Internetagentur Schott GmbH, 2010. All rights reserved.

3.3. Anschliessen des ADSL Kabels, Computers und Steckernetzteils

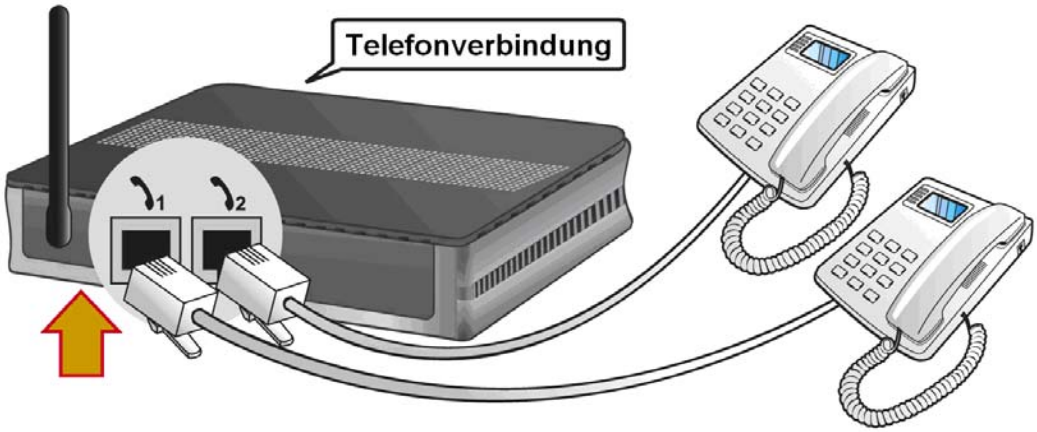
3.3.1. LAN Verbindung

Benutzen Sie das gelbe LAN Kabel. Schliessen Sie dieses auf der Rückseite des IADs an einer der vier gelben Ethernetschnittstellen an. Verbinden Sie das andere Ende des gelben Ethernetkabels mit Ihrem Computer.



3.3.2. Telefonverbindung

Verbinden Sie mit RJ-11 Kabeln Ihre analogen Telefone an den Anschlüssen Telefon 1 und Telefon 2 auf der Rückseite des IADs. Beide Anschlüsse können gleichzeitig VoIP Anrufe tätigen. Jedoch kann jeweils nur einer den Festnetzanschluss nutzen.



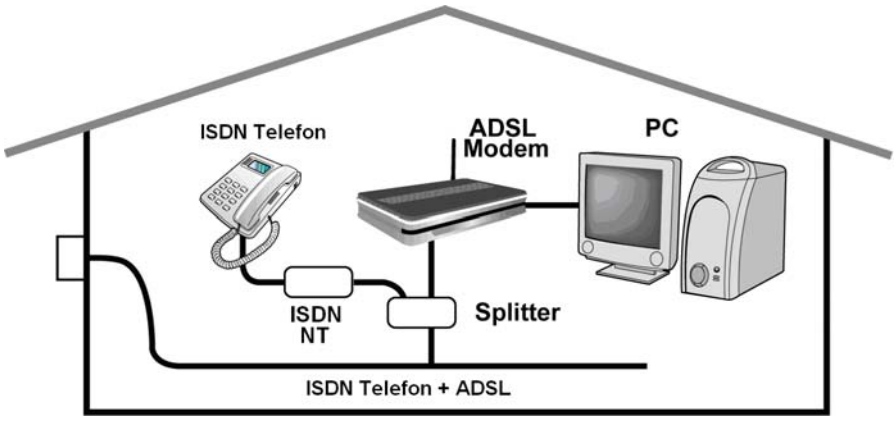
© Internetagentur Schott GmbH, 2010. All rights reserved.

3.3.3. Anschliessen des ADSL- und Festnetzkabels

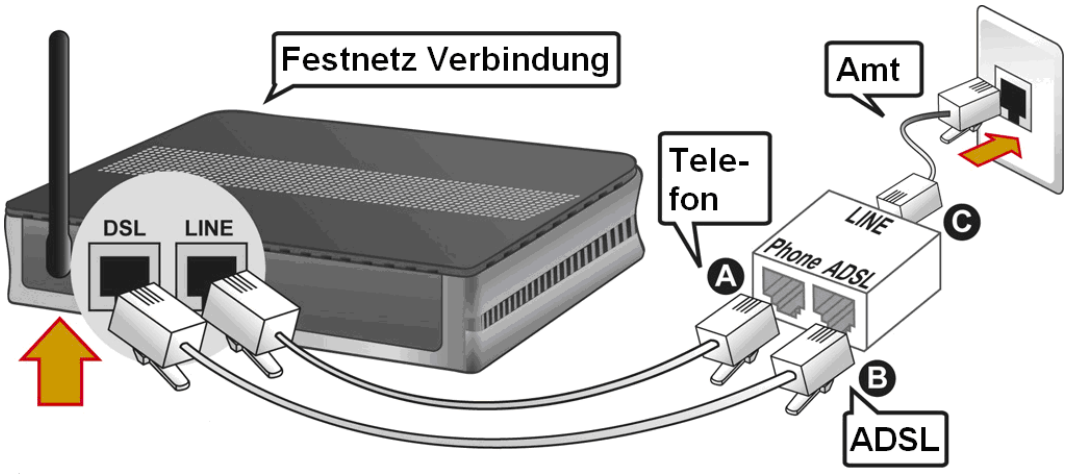
3.3.3.1 Splitter Verbindung (ISDN) → Entfällt bei Internet via Satellit

Der Splitter/Filter ist wichtig bei der ADSL-Installation, denn er führt die hohen Frequenzen zum IAD und die tiefen Frequenzen zum Telefon. Dadurch bleibt ihr Telefon vom ADSL-Signal unbeeinträchtigt und Ihr IAD wird eine stabile ADSL-Verbindung erhalten.

Wenn ADSL und ISDN kombiniert wird, ist ein Splitter notwendig. Dieser wird zentral vor dem ISDN NT angeschlossen. Schliessen Sie den Splitter der beigelegten Anleitung an.



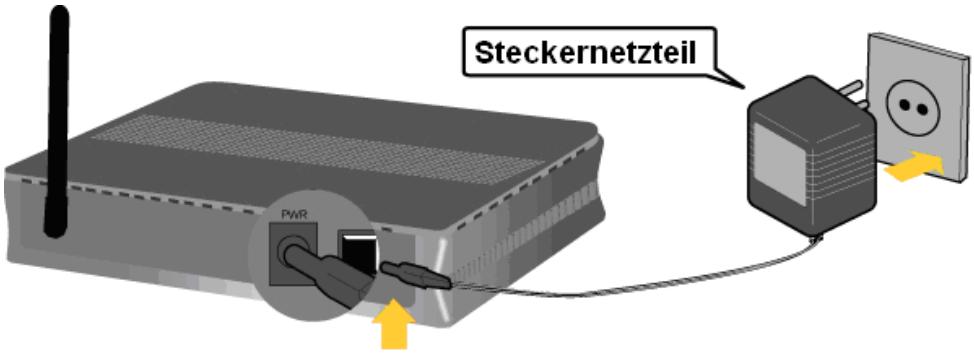
a) Verbinden Sie mit einem RJ-11 Kabel den ADSL Anschluss des IADs mit dem ADSL Anschluss am Splitter/Filter. (Entfällt bei Internet via Satellit)
b) Verbinden Sie mit dem mitgelieferten, schwarzen RJ-11 Kabel den Telefonanschluss „Line“ mit dem Telefonanschluss des Splitter/Filters.
c) Verbinden Sie den Amt-Anschluss des Splitter/Filters mit der Telefonsteckdose.



© Internetagentur Schott GmbH, 2010. All rights reserved.

3.3.4. Stromanschluss

Schliessen Sie das Steckernetzteil am Gerät an und stecken Sie es in die Steckdose.



3.4. Überprüfen der LEDs

Sobald Sie alle Kabel verbunden haben, schalten Sie das IAD durch Drücken des rückseitigen Ein-/Ausschaltknopfes ein. Nach zwei Minuten ist das Gerät bereit. Dies wird ebenfalls durch die Kontroll-LEDs auf der Gerätevorderseite angezeigt.

Nun sollten die unten eingekreisten LEDs leuchten.

© Internetagentur Schott GmbH, 2010. All rights reserved.

4. Aufrufen des Schnellstarts

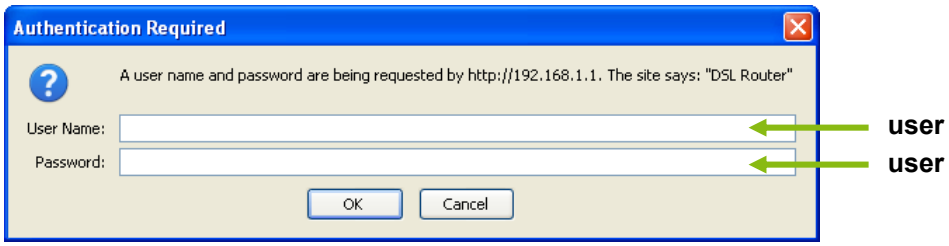
Öffnen Sie Ihren Internet Browser (z.B. Internet Explorer oder Firefox) und rufen Sie die Adresse 192.168.100.1 auf.
Sie werden aufgefordert Benutzername und Passwort anzugeben. Geben Sie als Benutzername **user** sowie als Passwort **user** ein.

Internet Explorer

Connect to 192.168.1.1
The server 192.168.1.1 at WebAdmin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel
user
user

Passworteingabe in Internet Explorer

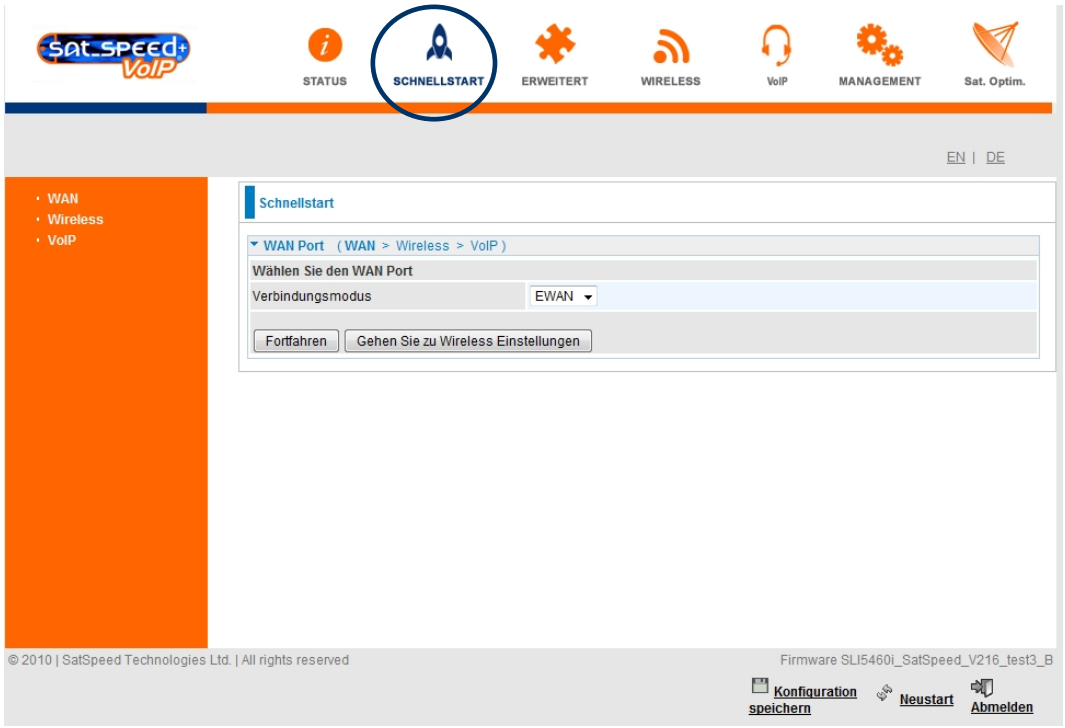
Firefox



Passworteingabe in Firefox

Sobald Sie durch klicken auf **OK** Ihre Eingabe bestätigen, werden Sie auf die folgende Seite geleitet.

© Internetagentur Schott GmbH, 2010. All rights reserved.

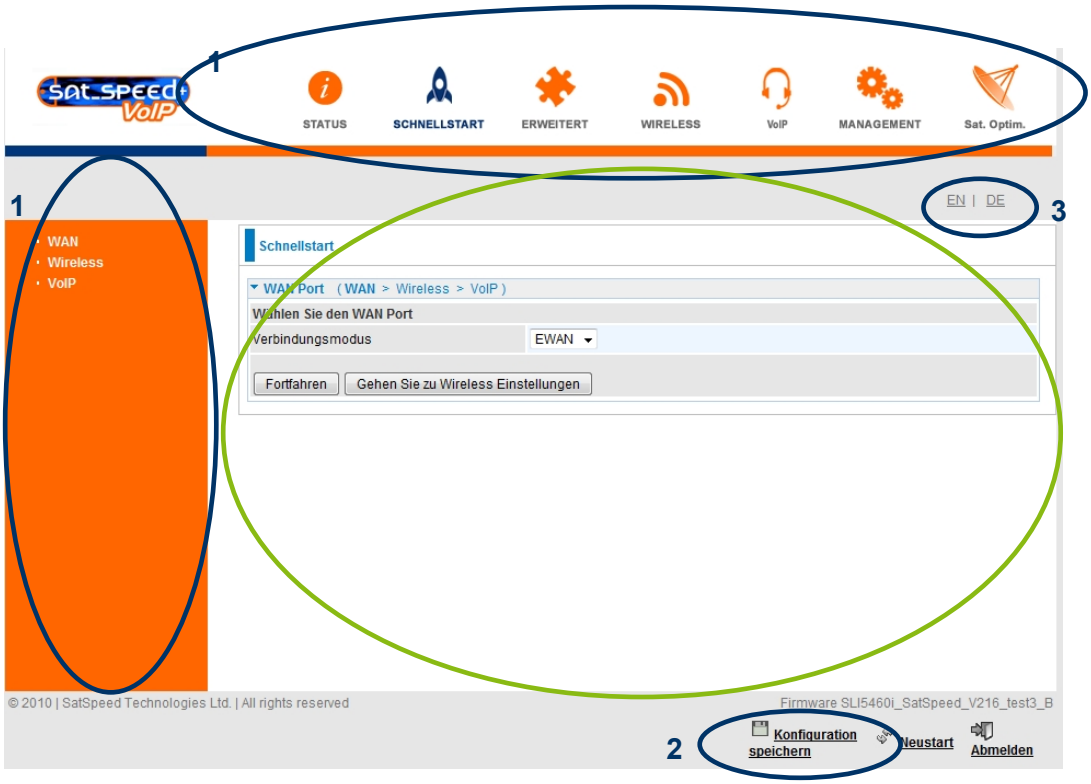


Klicken Sie auf „**Schnellstart**“, um Ihre Internetverbindung, Ihr Wireless LAN und Ihre Internet Telefonie zu konfigurieren.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5. Konfiguration

Das Web Interface ist unterteilt in das Navigationsmenü (eingekreist in blau, 1) und in die Inhaltsseite (eingekreist in grün) in welcher die Änderungen vorgenommen werden können.
Dieses Benutzerhandbuch erklärt jede einzelne Inhaltsseite.



Menüpunkte	Inhalt
Status	Informationen werden nur angezeigt, können nicht verändert werden.
Schnellstart	Einrichtungsassistent für Ihre Internet Verbindung, Wireless LAN und Internettelefonie (VoIP).
Erweitert	Weiterführende Einrichtungsmöglichkeiten für LAN, Internetverbindung, Sicherheitseinstellungen, Firewall, usw.
Wireless	Alle Einstellungen, die Ihr WLAN betreffen, finden Sie hier.
VoIP	Alle Einstellungen, die Ihre Internettelefonie betreffen, finden Sie hier.
Management	Verwaltungseinstellungen wie z.B. Zeiteinstellungen, Zugriffsrestriktionen, Firmware Update, usw.

Die Farbe des selektierten und somit aktiven Menüpunkt ist blau, die inaktiven Symbole sind grün.

Nachdem Sie Ihr Gerät konfiguriert haben, speichern Sie diese Einstellungen mit **Konfiguration speichern** (in der Abbildung oben eingekreist in blau, 2). Für eine detaillierte Erklärung wird auf Kapitel **5.7 Konfiguration speichern** verwiesen.

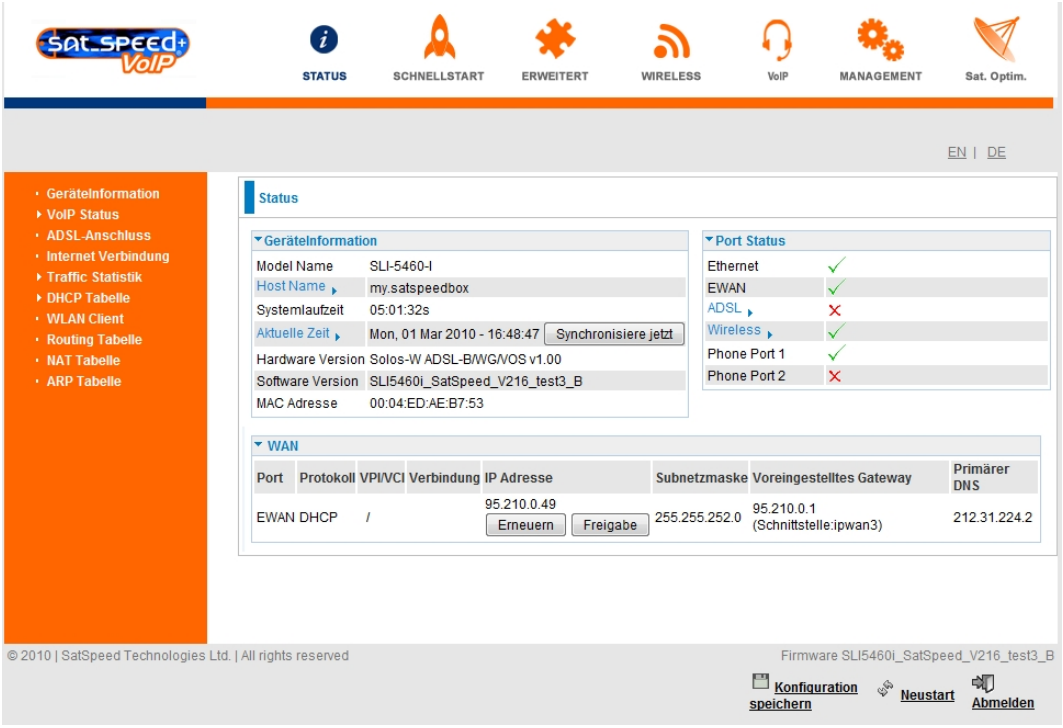
Das Gerät bietet verschiedene Sprachen zur Auswahl. Wählen Sie eine, indem Sie die entsprechende Verknüpfung wählen (in der Abbildung oben eingekreist in blau, 3).

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1. Status

5.1.1. Geräteinformation

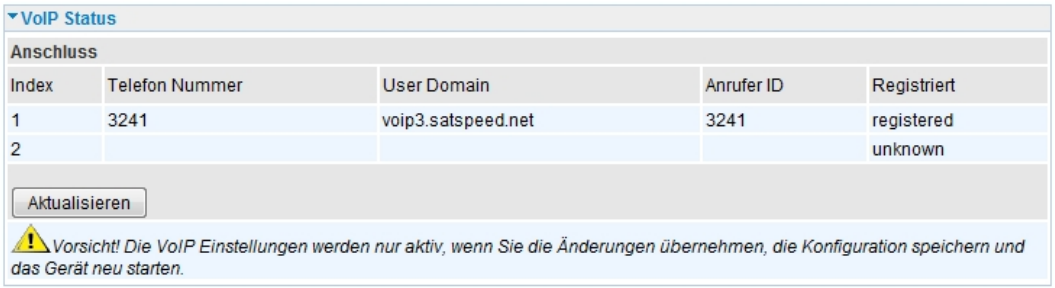
Diese Seite zeigt Informationen über das Gerät selbst, die Ports und Internetverbindung.



Geräte Information	Die Haupteigenschaften des Gerätes werden hier aufgelistet.
Port Status	Zeigt den Status der Anschlüsse / Buchsen / Ports. Ein grünes Häkchen steht für einen funktionierenden Anschluss. Ein rotes Kreuzchen für nicht verbunden / funktioniert nicht.
WAN	Die Haupteigenschaften der Internetverbindung stehen hier.

5.1.2. VOIP Status

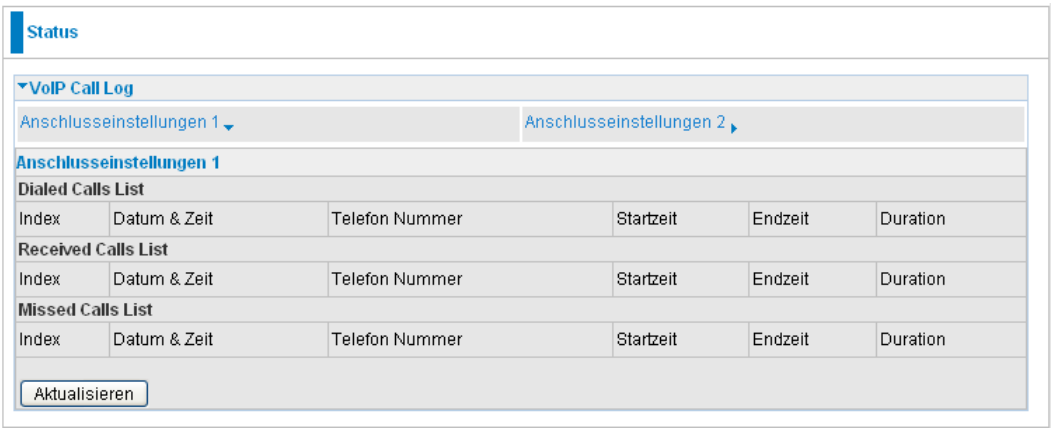
Diese Seite zeigt den Status der zwei angeschlossenen Telefone. Registriert heisst, dass an dem Anschluss über das Internet telefoniert werden kann (VoIP). Diese Seite wird nicht automatisch aktualisiert. Um ein Update des „Registriert“-Status zu erhalten, klicken Sie auf den **Aktualisieren** Knopf.


VoIP Status
Anschluss
Index Telefon Nummer User Domain Anrufer ID Registriert
1 3241 voip3.satspeed.net 3241 registered
2 unknown
Aktualisieren
Vorsicht! Die VoIP Einstellungen werden nur aktiv, wenn Sie die Änderungen übernehmen, die Konfiguration speichern und das Gerät neu starten.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1.2.1 Anrufliste

Auf dieser Seite können Sie Ihre Anrufliste sehen. Diese wird pro Telefonanschluss / Port geführt.

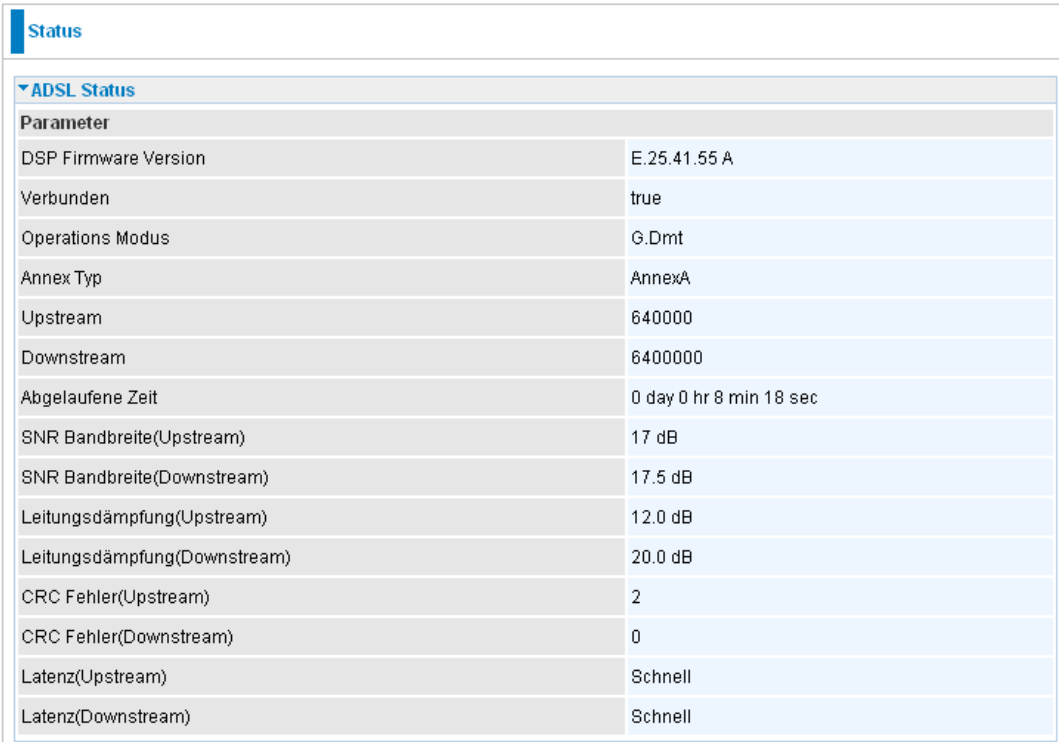


Dialled Calls List	Zeigt die letzten 10 gewählten Anrufe.
Received Calls List	Zeigt die letzten 10 erhaltenen Anrufe.
Missed Calls List	Zeigt die letzten 11 verpassten Anrufe.

Klicken Sie den **Aktualisieren** Knopf, um ein Update zu erhalten.

5.1.3. ADSL-Anschluss

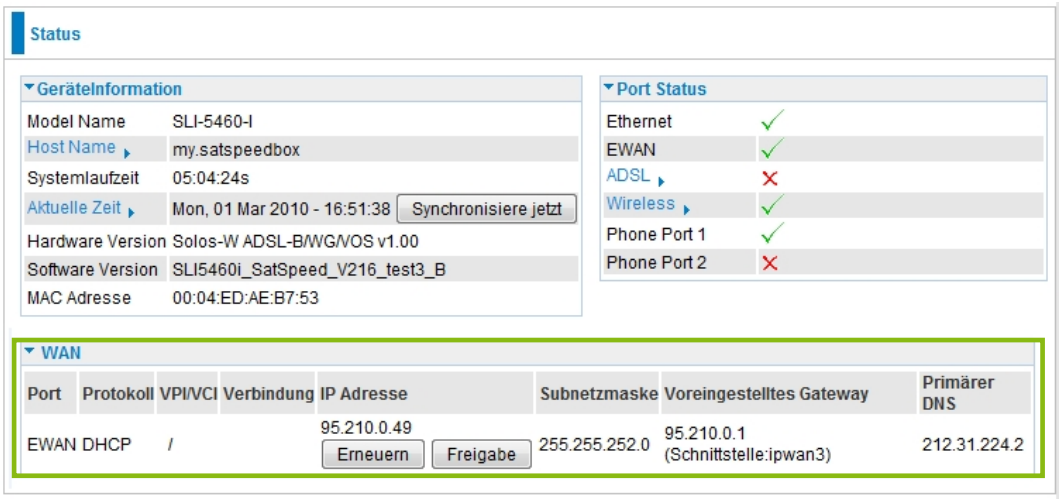
Diese Seite zeigt eine Gesamtübersicht des ADSL Status. Diese Seite ist zur Fehlerbehebung für Experten empfohlen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1.4. Internet Verbindung

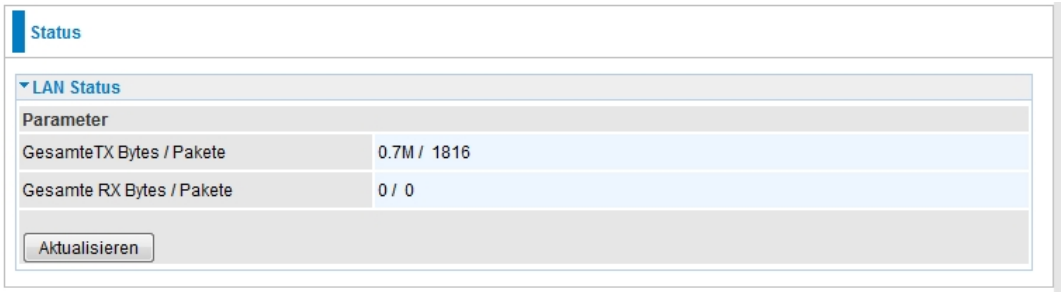
Der grün umrahmte Teil dieser Seite zeigt den Status der Internetverbindungen. Für detaillierte Infos wird auf Kapitel **5.1.1 Geräteinformation** verwiesen.



5.1.5. Traffic Statistik

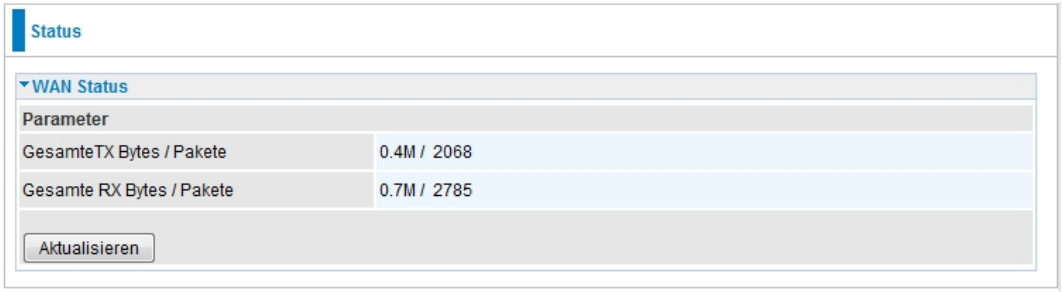
5.1.5.1 LAN Status

Diese Seite zeigt die gesendeten (TX) und den erhaltenen (RX) Bytes und Pakete an.



5.1.5.2 WAN Status

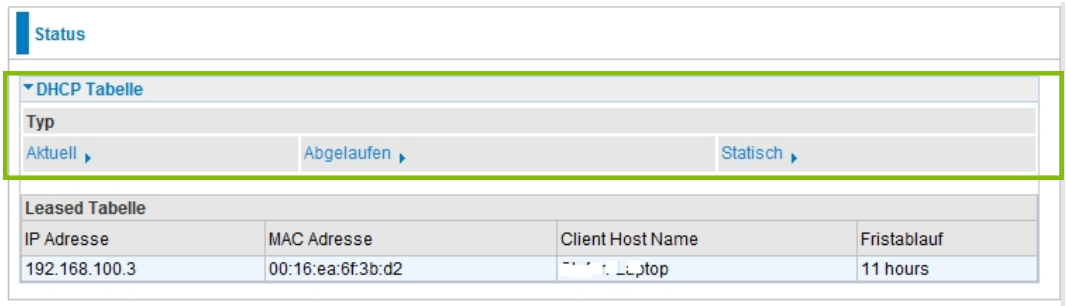
Für die detaillierte Beschreibung wird auf Kapitel **5.1.5.1 LAN Status** verwiesen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

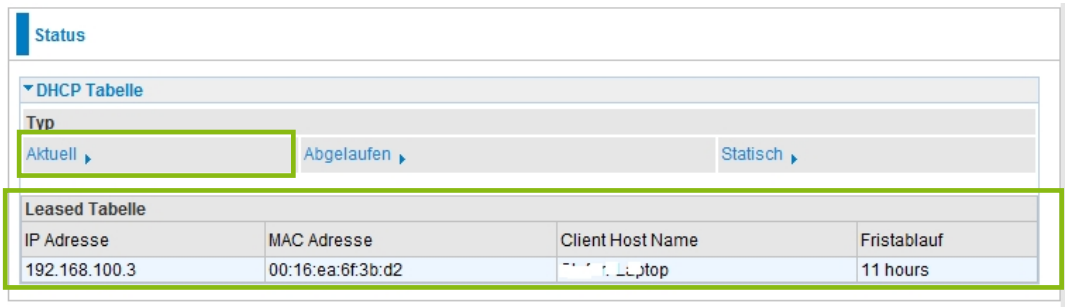
5.1.6. DHCP-Tabelle

Die DHCP-Tabelle listet alle Clients auf, die automatisch eine IP Adresse beziehen.
Bemerkung: Clients mit statischer IP Adresse werden nicht aufgelistet.



Aktuell	Die vom DHCP Server verteilten Adressinformationen.
Abgelaufen	Die abgelaufenen IP Adressinformationen.
Statisch	Die statischen IP Adressinformationen.

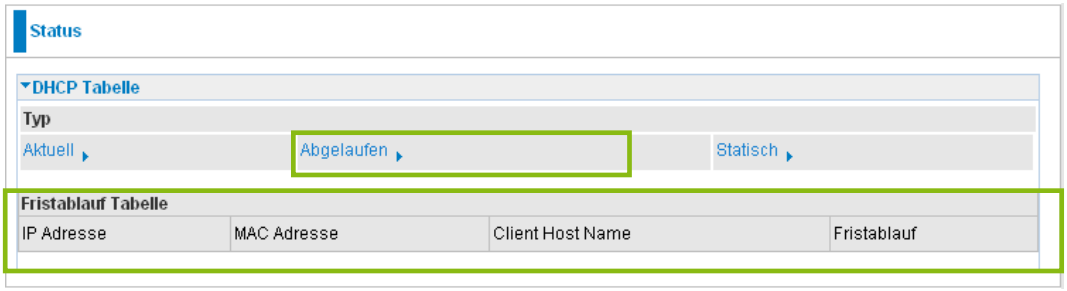
5.1.6.1 Aktuell



IP Adresse	Die einem Client zugewiesene IP Adresse.
MAC Adresse	Die MAC Adresse eines Clients.
Client Host Name	Der Host Name (Computername) eines Clients.
Fristablauf	Verbleibende Zeit, bis die IP Adresse abläuft und erneuert wird (wenn der Client aktiv ist) oder verfällt (wenn der Client nicht mehr verbunden ist).

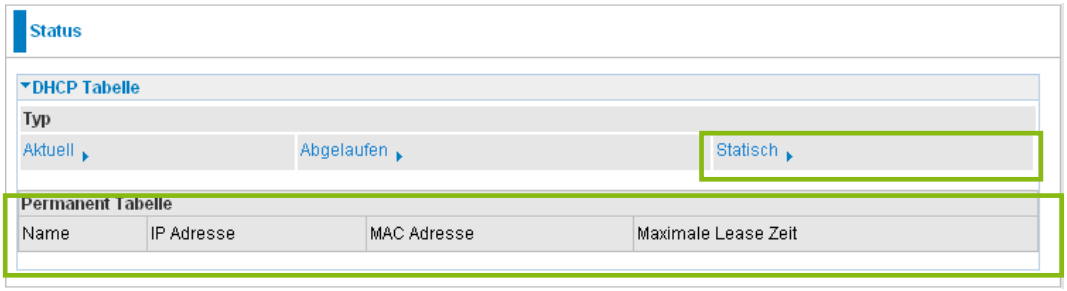
© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1.6.2 Abgelaufen



Diese Tabelle zeigt die abgelaufenen IP Adressen an, die neu verteilt werden können.

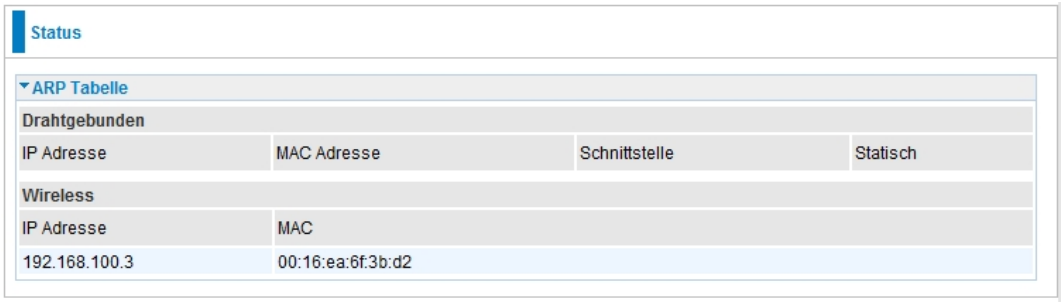
5.1.6.3 Statisch



Statische IP Adressen werden für bestimmte MAC Adressen reserviert. Demzufolge werden diese hier aufgelisteten IP Adressen keinem anderen Client zugewiesen.

5.1.7. WLAN Clients

Diese Seite zeigt die ARP (Address Resolution Protocol) Tabelle des Gerätes, welche die IP- und MAC Adressen beinhaltet. Diese Tabelle unterscheidet „Wired“ (kabelgebundene) und „Wireless“ (kabellose) Clients.

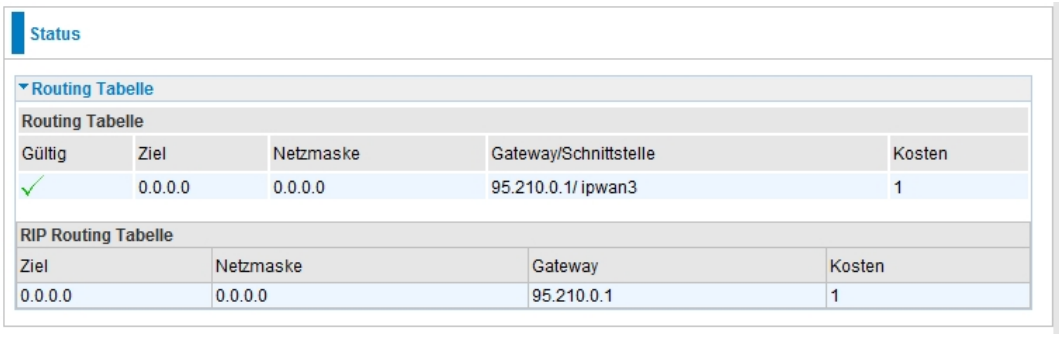


IP Adresse	Die Liste mit IP-Adressen der Geräte in Ihrem lokalen Netzwerk.
MAC Adresse	Die Liste mit MAC-Adressen der Geräte in Ihrem lokalen Netzwerk.
Schnittstelle	Die Schnittstelle mit welcher ein Client verbunden ist.
Statisch	„Statischer“ Status des ARP Tabelleneintrag: “**no**” für dynamisch generierte ARP Tabelleneinträge. “**yes**” für statische durch den Benutzer festgelegte ARP Einträge.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1.8. Routing Tabelle (Experten)

Die Routing Tabelle beschreibt den Weg, den Pakete bis zu Ihrem Bestimmungsort nehmen.



Routing Tabelle

Gültig	Zeigt einen erfolgreichen Routing Status an.
Ziel	IP Adresse des Zielnetzwerkes.
Netzmaske	Netzmaske des Zielnetzwerkes.
Gateway/Schnittstelle	IP Adresse des Gateways oder einer existierenden Schnittstelle, welche/r die Route braucht.
Kosten	Die Anzahl Hops werden unter Kosten aufgelistet.

RIP Routing Tabelle

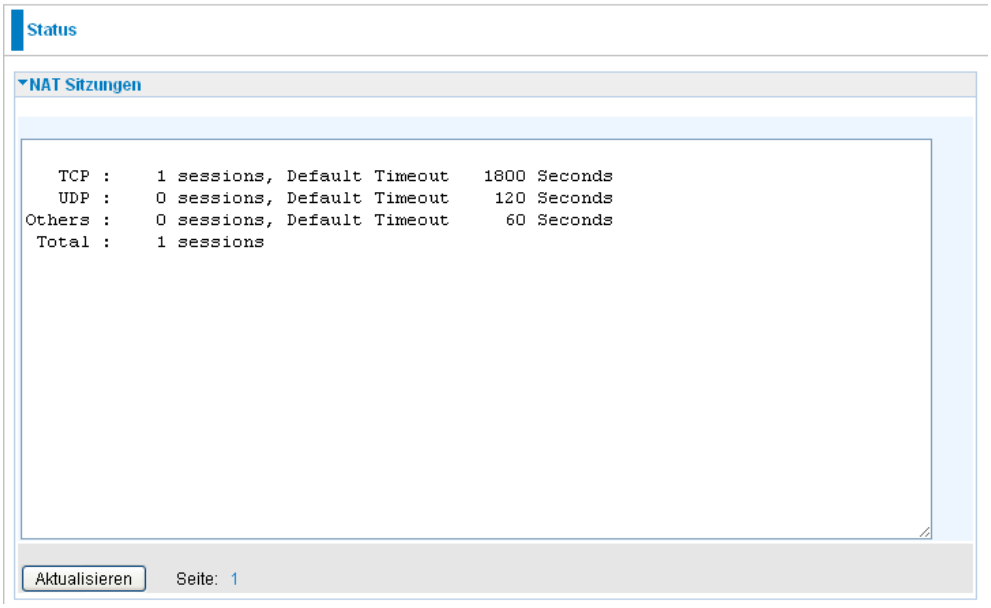
Ziel	IP Adresse des Zielnetzwerkes
Netzmaske	Netzmaske des Zielnetzwerkes.
Gateway	IP Adresse des Gateways, welcher die Route braucht.
Kosten	Die Anzahl Hops werden unter Kosten aufgelistet.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.1.9. NAT Tabelle (Experten)

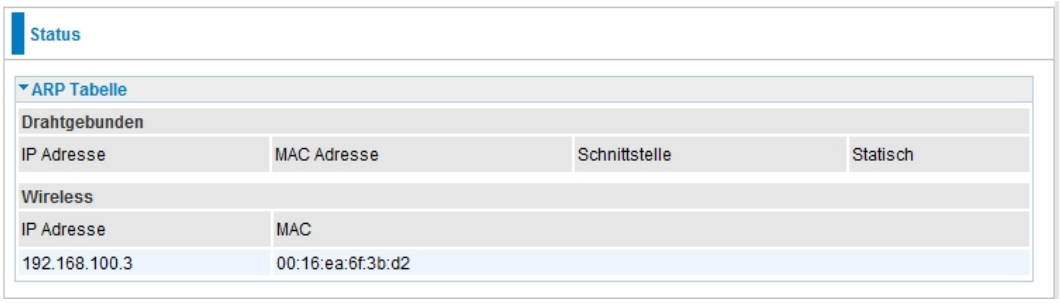
NAT (Network Address Translation) wird benötigt, um ein lokales Netzwerk unbekannter Grösse mit dem Internet zu verbinden und dabei nur eine einzige IP Adresse zu verwenden.

Diese Seite listet alle aktuellen NAT Sitzungen zwischen der WAN Schnittstelle des Geräts und dem LAN / WLAN auf.


Status
NAT Sitzungen
TCP : 1 sessions, Default Timeout 1800 Seconds
UDP : 0 sessions, Default Timeout 120 Seconds
Others : 0 sessions, Default Timeout 60 Seconds
Total : 1 sessions
Aktualisieren
Seite: 1

5.1.10. ARP-Tabelle

Für eine detaillierte Erklärung wird auf Kapitel **5.1.7 WLAN Clients** verwiesen.



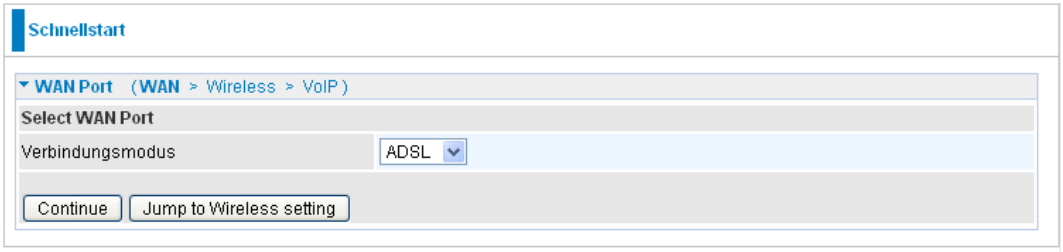
© Internetagentur Schott GmbH, 2010. All rights reserved.

5.2. Schnellstart

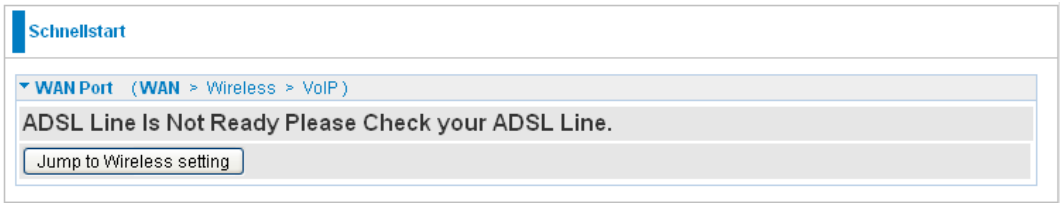
Einrichtungsassistent für Ihre Internet Verbindung, Wireless LAN und Internettelefonie (VoIP).

WAN (Internet Verbindung)

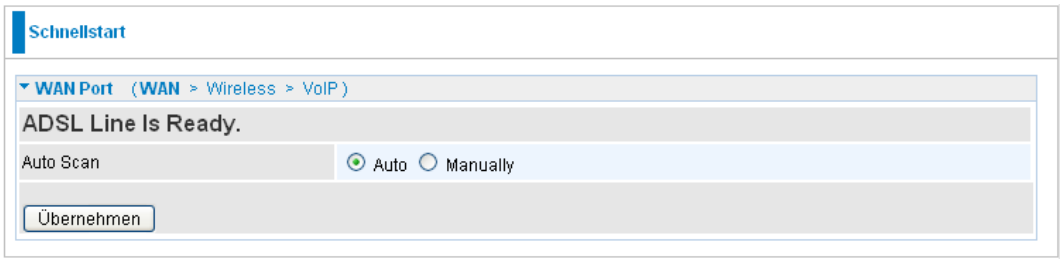
1. Klicken Sie **Schnellstart** und danach **Continue/ Weiter.**



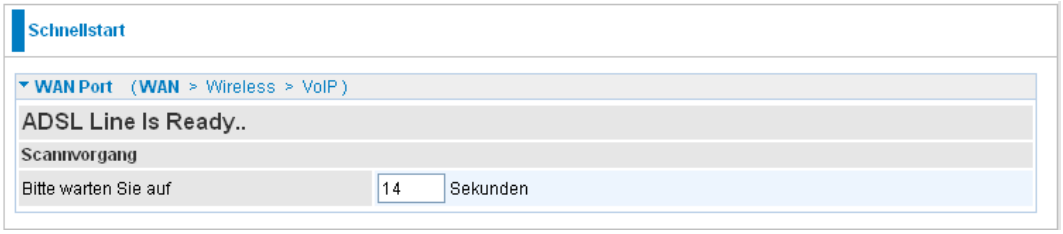
2. Wenn Ihre ADSL Verbindung nicht bereit ist, überprüfen Sie Ihr ADSL Kabel. Näheres dazu finden Sie im Kapitel **3.3.3 Anschliessen des ADSL- und Festnetzkabels.**



3. Wenn Ihre ADSL Verbindung bereit ist, erscheint die folgende Seite: **ADSL Line is Ready**. Wählen Sie den **Auto** Radio Button und klicken Sie **Übernehmen**.
Bemerkung: Wenn Sie **Manually** wählen, müssen Sie die ADSL Verbindung selbst einrichten (fahren Sie dann mit Punkt 5 weiter).

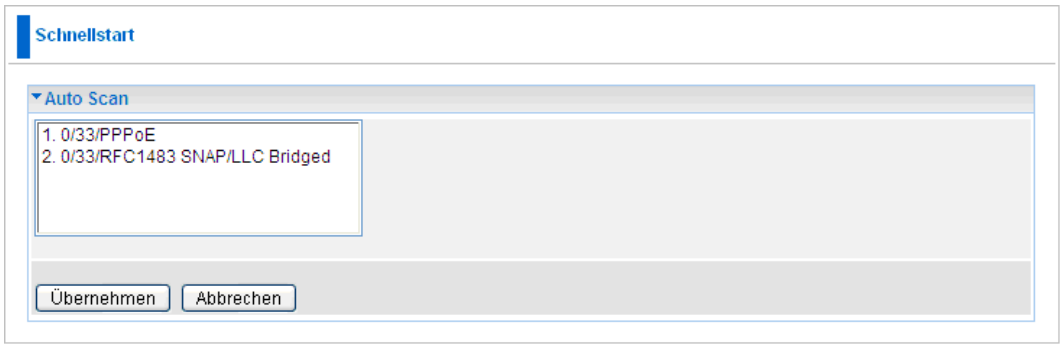


Es wird automatisch nach den verfügbaren Modi gesucht.

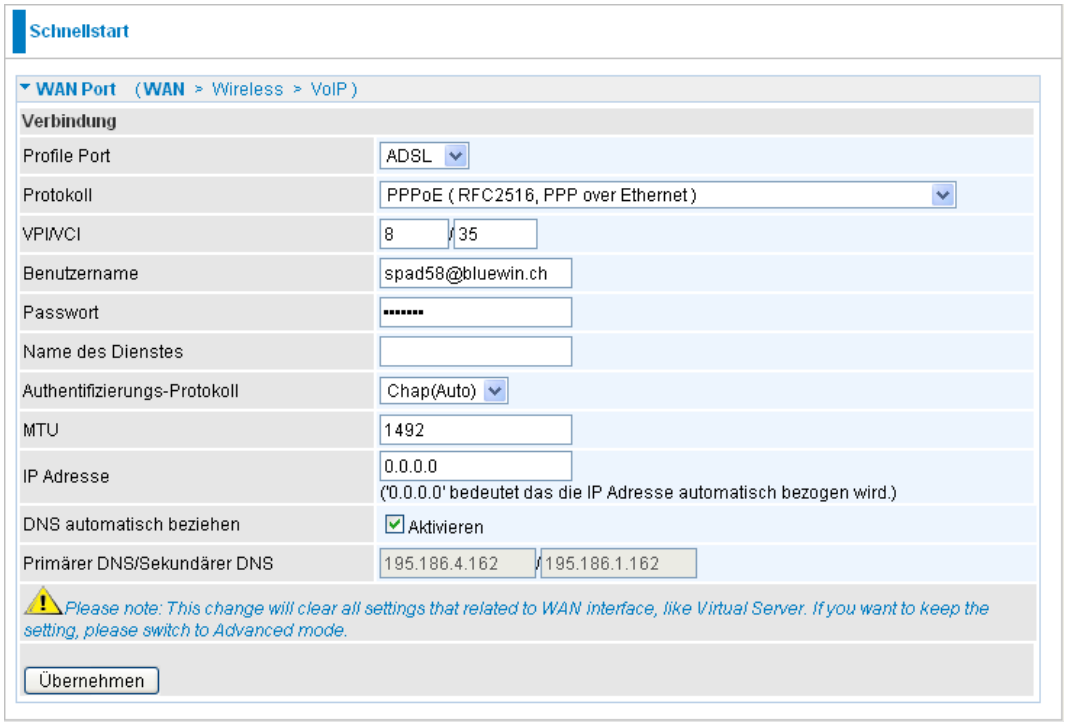


© Internetagentur Schott GmbH, 2010. All rights reserved.

4. In untenstehender Liste können Sie zwischen den verschiedenen Verbindungstypen wählen. Wählen Sie den von Ihrem ISP vorgegebenen Verbindungstyp und klicken Sie auf **Apply**.



5. Bitte geben Sie „**Benutzername**“ und „**Passwort**“ ein, um sich bei Ihrem ISP anzumelden und überprüfen Sie auch die anderen Felder. Klicken Sie auf **Übernehmen**, um fortzufahren.

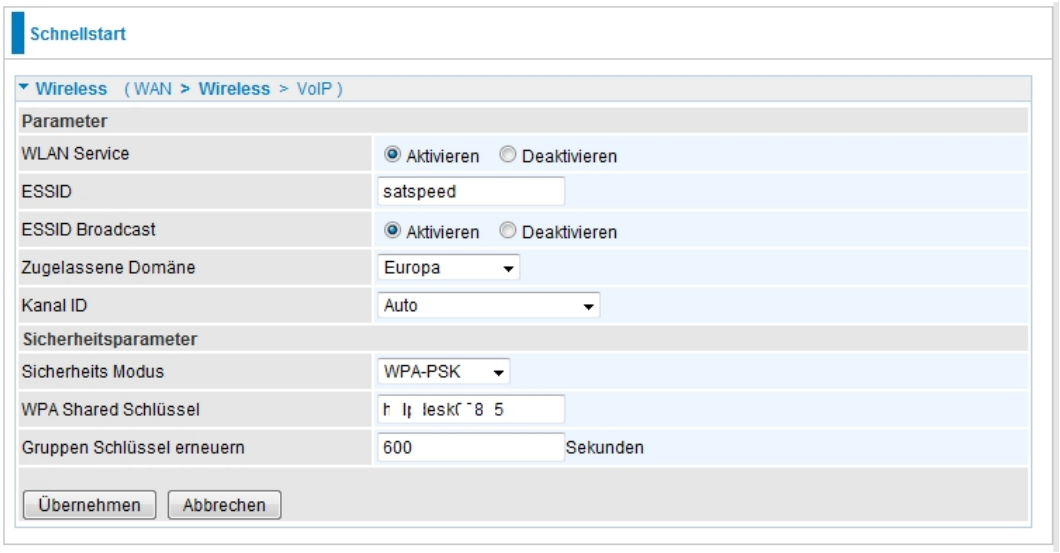


Profile Port	Wählen Sie die Verbindungsart. Zum Beispiel: ADSL.
Protokoll	Wählen Sie die Protokollart. Voreingestellt ist PPPoE.
VPI/VCI	Geben Sie den vom ISP vorgegebenen VPI/VCI ein.
Benutzername	Geben Sie den vom ISP vorgegebenen Benutzernamen ein.
Passwort	Geben Sie das vom ISP vorgegebene Passwort ein.
Name des Dienstes	Wird zu Identifikationszwecken gebraucht. Falls nötig, wird er Ihnen vom ISP mitgeteilt.
Authentifizierungs-Protokoll	Voreingestellt ist **Auto**. Ihr ISP gibt vor, welche Auswahl (**Chap** oder **Pap**) Sie treffen müssen.
IP Adresse	Ihre WAN IP Adresse. Lassen Sie diese auf 0.0.0.0, um automatisch eine IP Adresse von Ihrem ISP zu beziehen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

WLAN

6. Konfigurieren Sie die Wireless LAN Einstellungen.

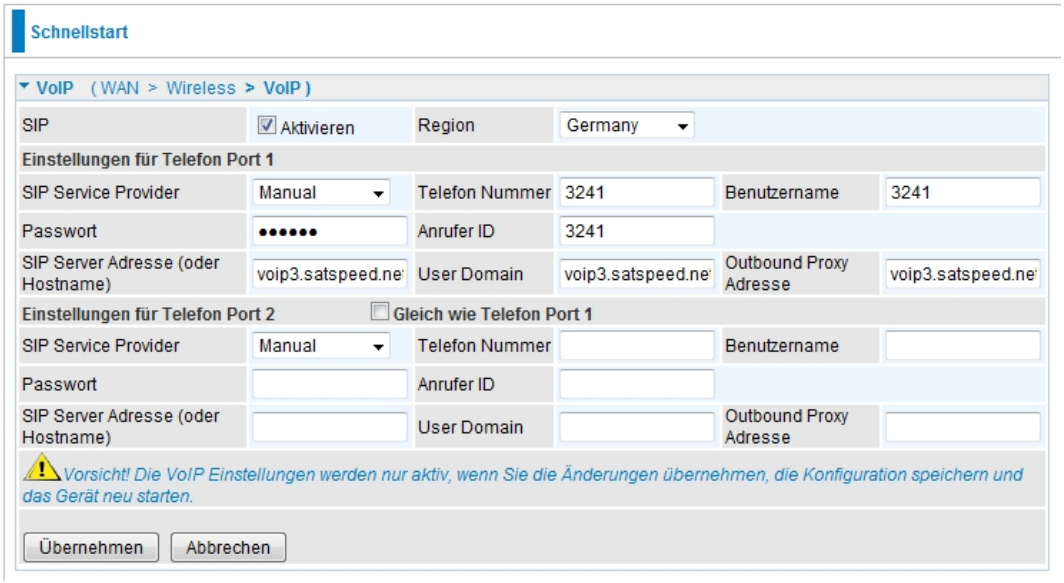


WLAN Service	Voreingestellt ist **Deaktivieren**. Wenn Sie eine Wireless Verbindung nutzen möchten, wählen Sie **Aktivieren**.
ESSID	Die ESSID ist der eindeutige Name des Wireless Access Point (AP). Es wird zwischen Gross- und Kleinschreibung unterschieden und der Name darf nicht länger als 32 Zeichen sein. Stellen Sie sicher, dass Ihre Clients dieselbe ESSID wie das Gerät verwenden, damit sie sich mit Ihrem Wireless Netzwerk verbinden können.
ESSID Broadcast	Voreingestellt ist **Aktivieren**. **Aktivieren:** Ihre ESSID ist sichtbar für andere WLAN Clients. **Deaktivieren:** Ihre ESSID ist unsichtbar für andere WLAN Clients.
Zugelassene Domäne	Sie können Ihr Land auswählen. Das ausgewählte Land bestimmt die zugelassenen Kanäle.
Kanal	Wählen Sie den Kanal, den Sie benutzen möchten.
Sicherheits Modus	Der voreingestellte Modus für die Wireless Sicherheit ist **WPA-PSK**. Sie können die Wireless Sicherheit ausschalten oder mit WPA-PSK, WPA2-PSK oder WEP einschalten. Es wird empfohlen die Wireless Sicherheit einzuschalten, um ihr Netzwerk zu schützen.
WPA Shared Schlüssel	Ein eindeutiger WPA Shared Schlüssel ist voreingestellt (Sie finden ihn auf dem Kleber auf der Unterseite des Gerätes). Falls Ihnen dieser nicht genügt, können Sie ihn ändern.
Gruppen Schlüssel erneuern	Wenn Sie WPA als Sicherheitsmodus wählen, dann ändern das Gerät und die WLAN Clients den Schlüssel periodisch und automatisch.

© Internetagentur Schott GmbH, 2010. All rights reserved.

VoIP

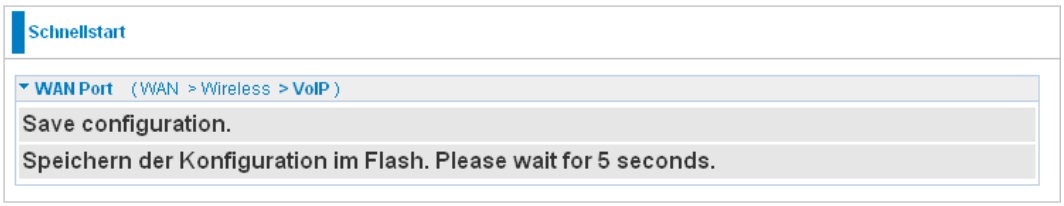
7. Einrichtung der Internettelefonie



SIP	Voreingestellt ist **Deaktivieren**. Aktivieren Sie die Checkbox um die Internettelefonie zu aktivieren.
Region	Wählen Sie das Land, in welchem Sie das Gerät benutzen.
SIP Service Provider	Wählen Sie Ihren SIP Service Provider und einige Felder werden automatisch ausgefüllt. Wählen Sie **Manual**, wenn Ihr SIP Service Provider nicht aufgelistet ist.
Telefon Nummer	Diese Felder sind von Ihrem SIP Service Provider vorgegeben, füllen Sie sie entsprechend aus.
Benutzername	
Passwort	
Anrufer ID	Dieser Name wird am Telefon des Angerufenen angezeigt.

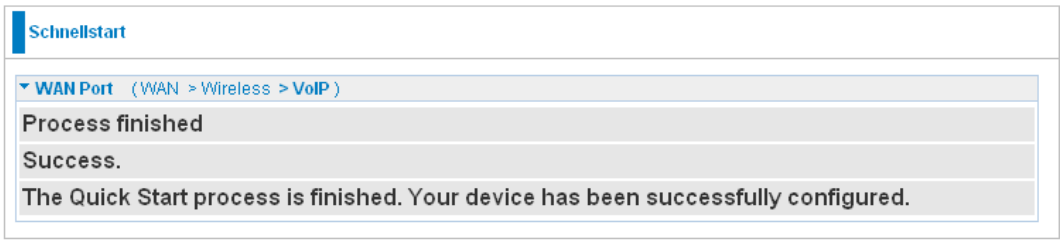
Klicken Sie auf **Übernehmen**, wenn Sie die Einstellungen eingegeben haben.

8. Warten Sie, bis die Konfiguration abgespeichert ist.


Schnellstart
WAN Port (WAN > Wireless > VoIP)
Save configuration.
Speichern der Konfiguration im Flash. Please wait for 5 seconds.

© Internetagentur Schott GmbH, 2010. All rights reserved.

9. Bei erfolgreicher Konfiguration wird die folgende Seite angezeigt:


Schnellstart
WAN Port (WAN > Wireless > VoIP)
Process finished
Success.
The Quick Start process is finished. Your device has been successfully configured.

Klicken Sie in der Navigationsleiste auf **Status**, um ihre ADSL Verbindung und VoIP Registration zu überprüfen.

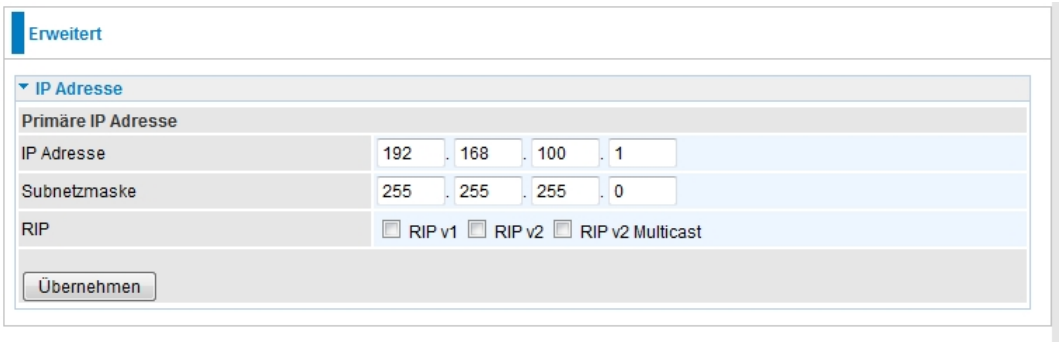
© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3. Erweitert

Die Konfigurationsoptionen im **Erweitert** Menü sind für diejenigen erfahrenen Benutzer, die die Vorteile des Gerätes bis ins Detail ausnutzen möchten. Wenn Sie hier Änderungen vornehmen, sollten Sie Ihre aktuelle Konfiguration auf Ihrem Computer speichern (dazu wird auf **5.6.10 Backup Konfiguration** verwiesen).

5.3.1. Lokales Netzwerk

5.3.1.1 IP Adresse



Primäre IP Adresse

IP Adresse	Die Standard IP Adresse des Gerätes.
Subnetzmaske	Die Standard Subnetmaske des Gerätes.
RIP	RIP v1, RIP v2, und RIP v2 Multicast. Wählen Sie die entsprechende Funktion, indem Sie die entsprechende Checkbox aktivieren.

5.3.1.2 DHCP Server

Der DHCP Server (Dynamic Host Configuration Protocol) weist den Computern in Ihrem Netzwerk automatisch eine IP Adresse zu, vorausgesetzt diese sind entsprechend konfiuriert. Dazu wird auf Kapitel **3.2 Konfigurieren des PCs (TCP / IP Einstellungen)** verwiesen.
Sie können den DHCP Server sowie auch die DHCP Relay Funktion aktivieren oder deaktivieren.

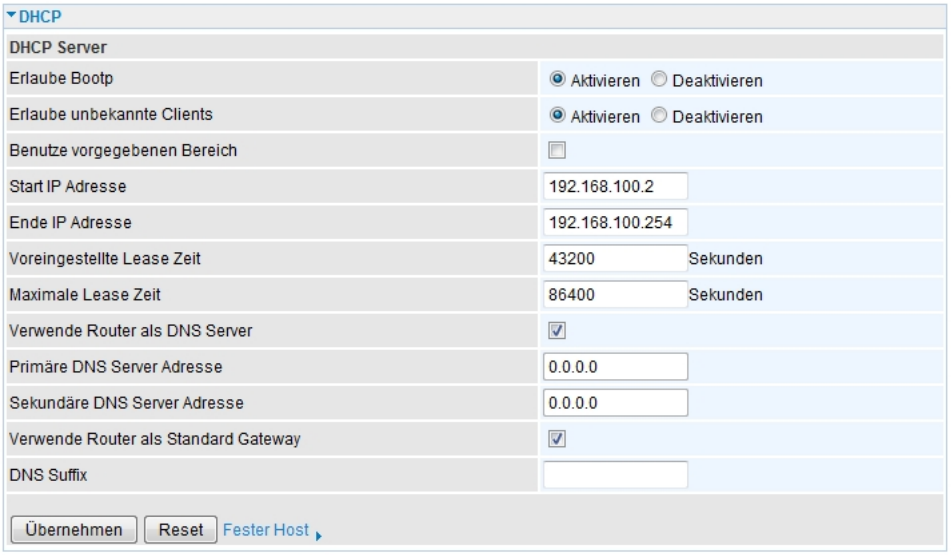
Deaktiviert	Wenn Sie alle IP Adressen manuell vergeben möchten, können Sie den DHCP Server deaktivieren. Um den DHCP Server des Gerätes zu deaktivieren, klicken Sie auf **Deaktivieren**, **Weiter** und danach auf **Bestätigen**. Wenn der DHCP Server ausgeschaltet ist, müssen Sie jedem Client im Netzwerk manuell eine statische IP Adresse zuweisen und das Standard Gateway für jeden Computer auf die IP Adresse des Gerätes (standardmässig 192.168.100.1) setzen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

DHCP Server

Ein DHCP Server macht eine Konfigurationen Ihrer Netzwerk Clients (Computer, Laptops, PDAs, Smartphones, etc.) einfacher, da diese automatisch konfiguriert werden.

Um den DHCP Server des Gerätes zu konfigurieren, wählen Sie **DHCP Server** und klicken Sie auf **Weiter**. Danach erscheint folgende Seite.



Hier können Sie die DHCP Parameter konfigurieren.
Diese beinhalten:

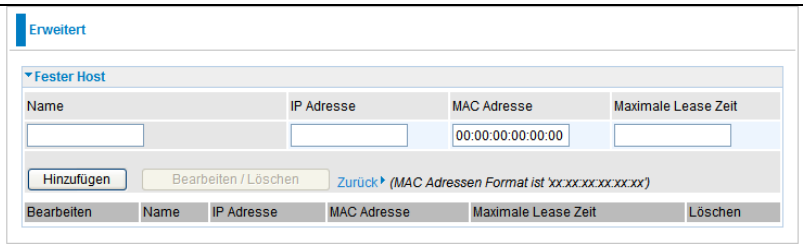
- Den IP Adresspool (Start und End IP Adresse, welche den Computern im Netzwerk zugewiesen werden).
- Die Fristablaufzeit jeder verteilten IP Adresse (d.h. die Zeitspanne, für die die IP Adresse gültig ist).
- Die primären und sekundären DNS Server Adressen.
- Die Gateway IP Adresse.

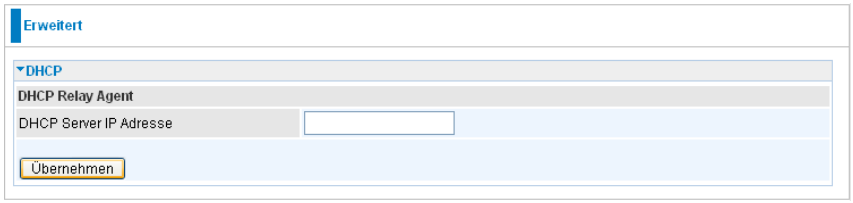
Diese Details werden dem DHCP Client (z.B. Ihrem Computer) geschickt, sobald dieser eine IP Adresse vom DHCP Server beziehen möchte.
Wenn Sie **Verwende Router als DNS Server** auswählen, sucht das Gerät die zum Domänenname gehörende IP Adresse ausserhalb des Netzwerkes automatisch und liefert die Antwort zurück zum anfordernden Computer im LAN.

Wenn Sie auf **Übernehmen** klicken, werden die Änderungen gespeichert.

Ausserdem finden Sie einen Text Link neben den Buttons am Ende der Seite. Diese Verknüpfung führt Sie zu DHCP Server – Fester Host.

© Internetagentur Schott GmbH, 2010. All rights reserved.

DHCP Server – Fester Host	 Diese Seite ermöglicht bestimmten nicht konfigurierten Netzwerkclients eine statische IP zuzuweisen. Allerdings muss dafür die MAC-Adresse des entsprechenden Computers bereits bekannt sein. Diese Funktion sollte von Clients verwendet, die entweder Port Forwarding benutzen (sehen Sie Kapitel: **5.3.4.1 Port Forwarding**) oder als DMZ Host agieren (sehen Sie Kapitel: **5.3.4.4 DMZ Host**)

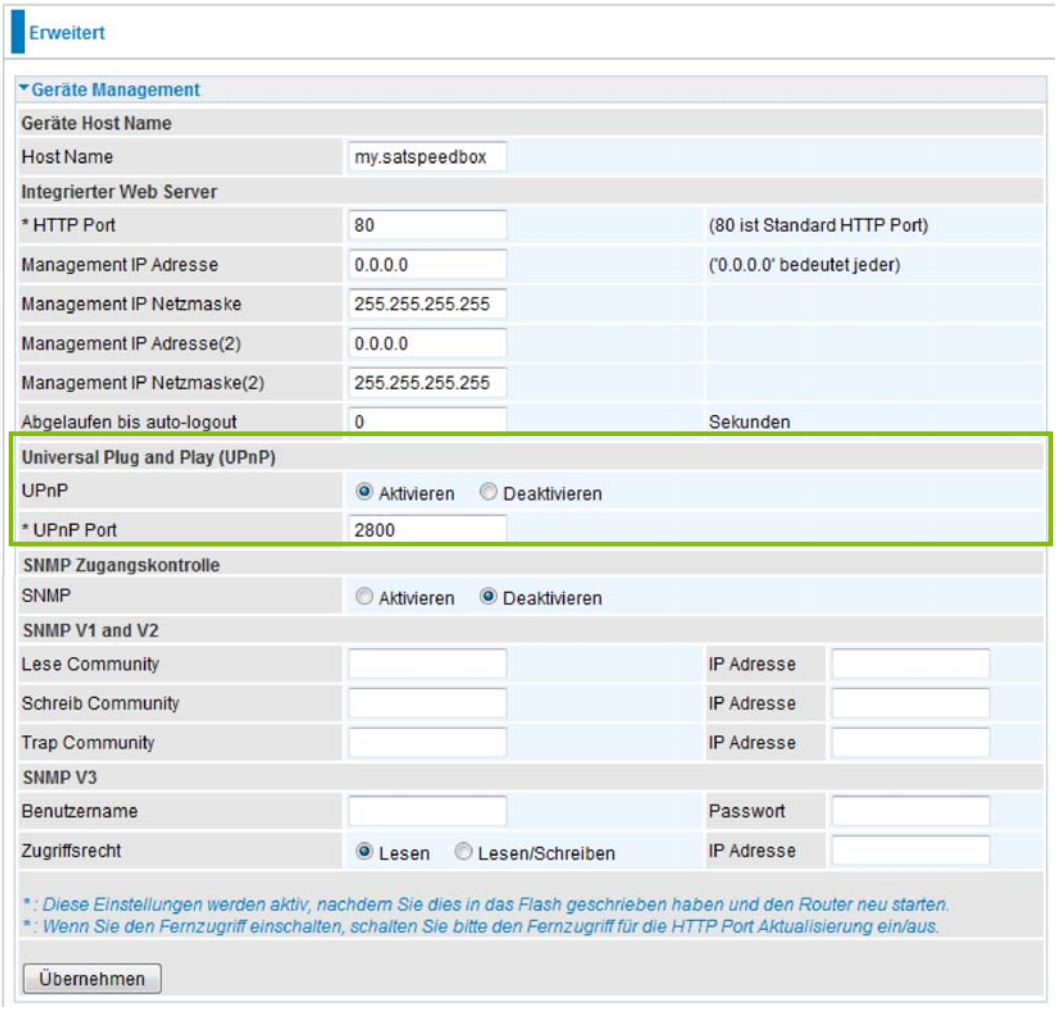
DHCP Relay Agent	Die DHCP Relay Agent Funktion erlaubt es Ihnen, das Gerät so zu programmieren, dass Sie einen externen DHCP Server in Ihrem LAN benutzen können. Wenn Sie **DHCP Relay Agent** auswählen und auf **Weiter** klicken, sehen Sie folgende Seite:  Hier können Sie die IP Adresse des DHCP Servers eingeben, welcher die IP Adressen im LAN den Clients zuweist. Wenn Sie auf **Übernehmen** klicken, wird der DHCP Relay Agent aktiviert.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.1.3 UPnP (Experten)

Geräte, die UPnP unterstützen, machen ihre Konfiguration automatisch.
UPnP bietet eine Peer-to-Peer Netzwerk Verbindung für Computer und andere Netzwerkgeräte. Dies wiederum ermöglicht Kontrolle und Datentransfer zwischen den Geräten. UPnP bietet viele Vorteile für Benutzer, die NAT Router via UPnP NAT Traversal benutzen.

Zusätzlich zum Gerät, müssen sowohl das Betriebssystem wie auch die Applikationen des Computers UPnP unterstützen. Windows XP unterstützt standardmässig UPnP (wenn die Komponente installiert ist). Windows 2000 unterstützt kein UPnP.

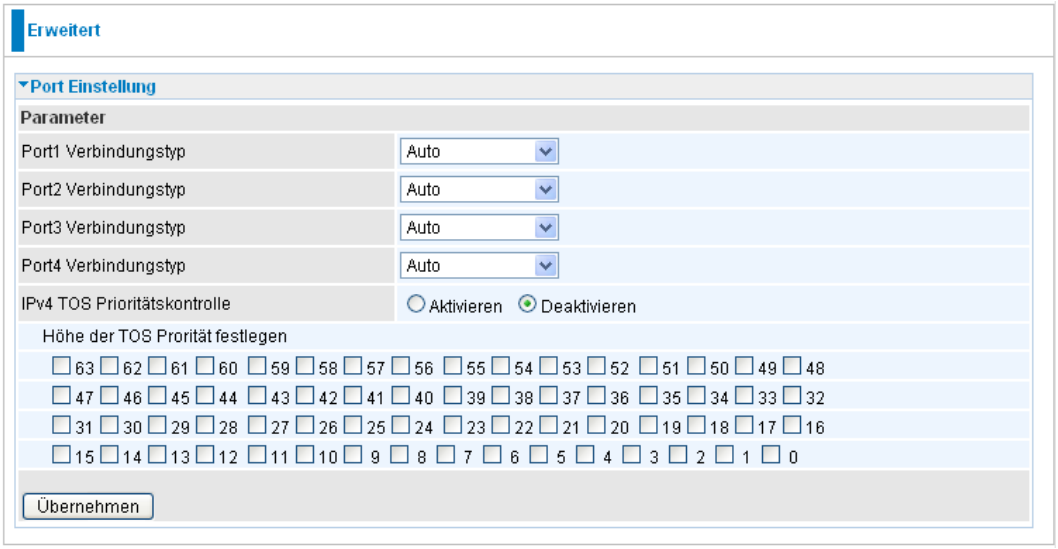


UPnP	**Deaktivieren:** Wählen Sie dies aus, um die UPnP Gerätefunktionalität zu deaktivieren. **Aktivieren:** Wählen Sie dies aus, um die UPnP Gerätefunktionalität zu aktivieren.
UPnP Port	Voreingestellt ist **2800**. Es wird empfohlen, diesen Port zu benutzen. Wenn dieser Wert allerdings bereits benutzt wird, können Sie ihn hier ändern.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.1.4 Port Einstellung (Experten)

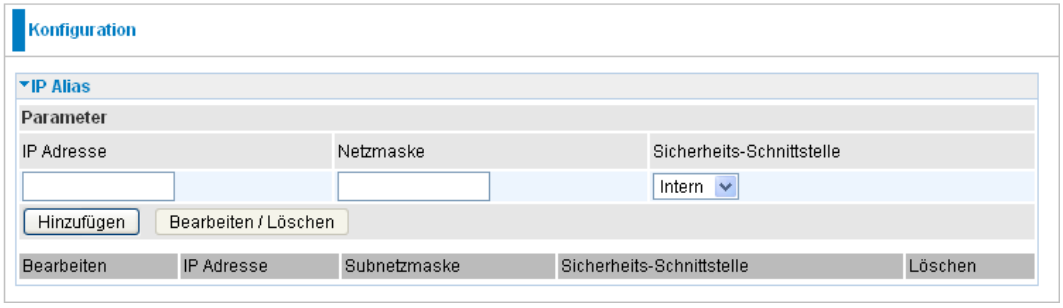
Diese Seite erlaubt Ihnen, im Falle eines Kompatibilitätsproblems oder für Performancesteigerungen des Netzwerkes, Einstellungen der Ethernet Ports vorzunehmen.


Erweitert
Port Einstellung
Parameter
Port1 Verbindungstyp
Auto
Port2 Verbindungstyp
Auto
Port3 Verbindungstyp
Auto
Port4 Verbindungstyp
Auto
IPv4 TOS Prioritätskontrolle
Aktivieren
Deaktivieren
Höhe der TOS Prorität festlegen
63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48
47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Übernehmen

Port # Verbindungstyp	Voreingestellt ist **Auto**, was Sie nicht ändern sollten, es sei denn, es treten bestimmte Probleme auf (z.B. wenn Ihre Computer nicht auf das LAN zugreifen können).
IPv4 TOS Prioritätskontrolle	TOS (Type of Services) wird benutzt, um die Priorität der Pakete festzulegen. Wenn das Paket eine hohe Priorität hat, wird es als erstes gesendet und die Geschwindigkeitsbegrenzung wird nicht berücksichtigt. Folglich wird der Ethernet Switch des Gerätes bei eingeschalteter Funktion das TOS Feld jedes IP Paketes und dessen enthaltenen Wert mit dem der oben aufgeführten Tabelle (0 bis 63) vergleichen. Wenn die Werte übereinstimmen, wird das Paket hoch priorisiert behandelt.

5.3.1.5 IP Alias (Experten)

IP Alias wird benutzt, um zusätzliche Netzwerkbereiche zu konfigurieren. Diese Netzwerkbereiche sind aber eine Einheit und reagieren als solche.

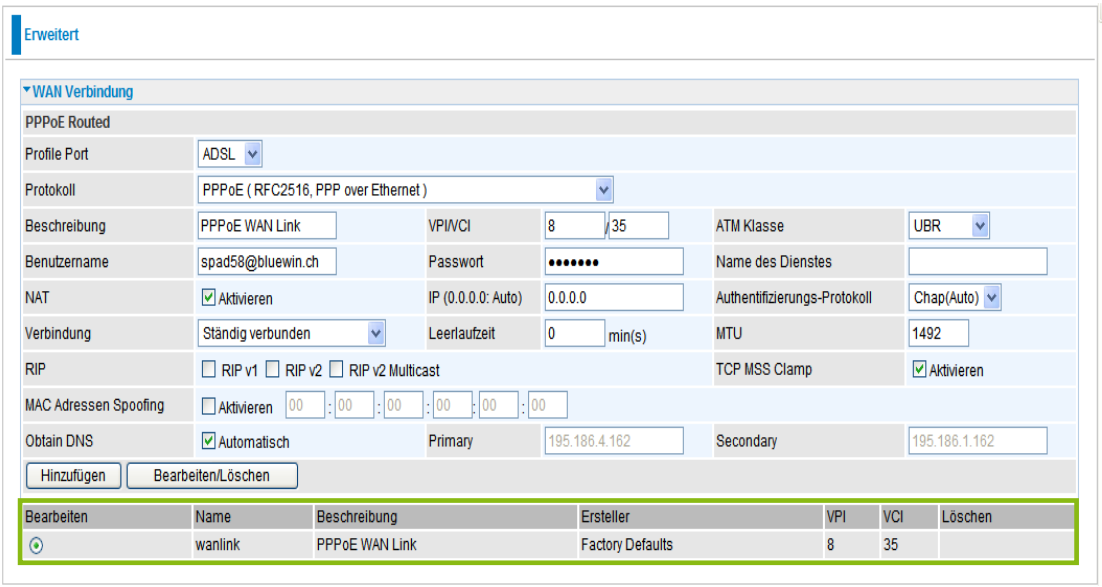


© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.2. Internet (Experten)

5.3.2.1 Verbindungen

Der eingerahmte Teil auf der folgenden Abbildung zeigt alle konfigurierten LAN Verbindungen. Wenn Sie eine WAN Verbindung mittels **Bearbeiten** Radio Button wählen, werden die entsprechenden Details angezeigt.

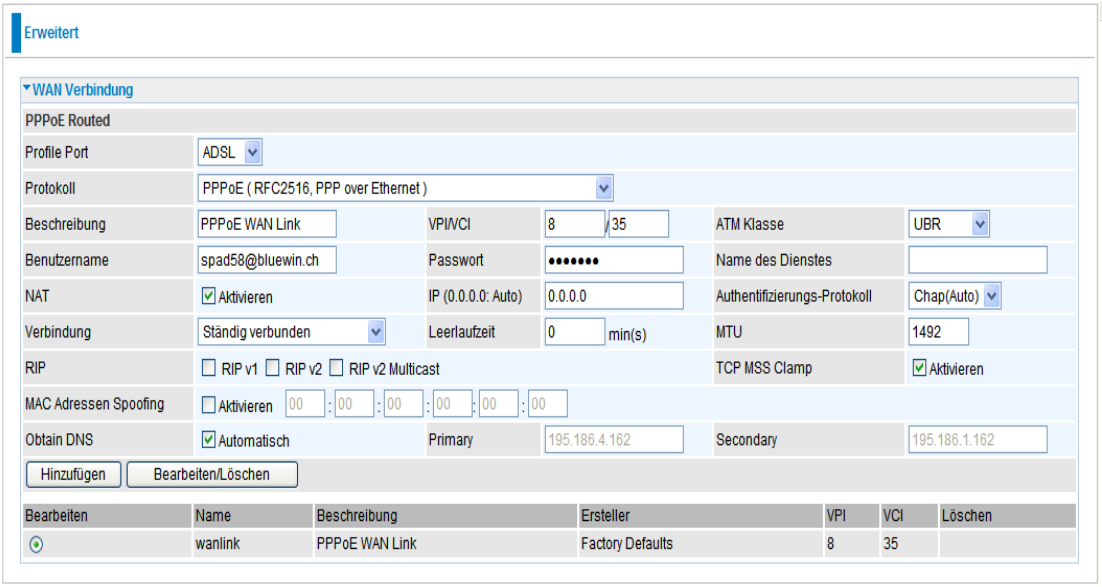


Um eine neue Verbindung hinzuzufügen, definieren Sie deren Einstellungen und klicken Sie auf **Hinzufügen**.
Um Änderungen bestehender Verbindungen zu bestätigen, klicken Sie auf **Bearbeiten/Löschen**.
Um eine Verbindung zu löschen, wählen Sie den **Löschen** Radio Button aus und klicken Sie auf **Bearbeiten/Löschen**.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.2.1.1. ADSL – PPPoE Verbindung

Das Protokoll (Verbindungstyp) PPPoE benutzt Einstellungen, die auch von anderen Protokollen benutzt werden. Folglich wird bei der Erklärung anderer Protokolle auf PPPoE verwiesen.



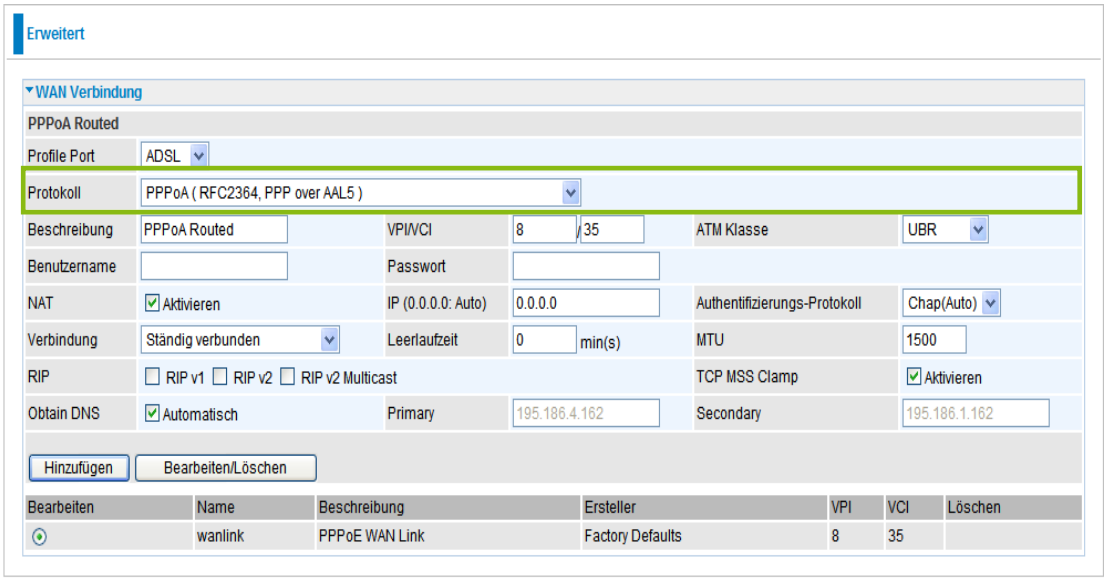
Profile Port	Wählen Sie ADSL. Damit wird der ADSL Anschluss auf der Rückseite des Gerätes benutzt. EWAN benutzt den Ethernet Anschluss 1, um eine Verbindung aufzubauen.
Protokoll	Das ATM Protokoll wird im Gerät benutzt.
Beschreibung	Ein vom Benutzer vergebener Name für die Verbindung.
VPI/VCI	Geben Sie die von Ihrem ISP angegebenen Daten ein.
ATM Klasse	Die Quality of Service für die ATM Schicht. Geben Sie die von Ihrem ISP angegebenen Daten ein.
Benutzername	Geben Sie den Benutzernamen ein. Sie können bis zu **128** alphanumerische Zeichen (Gross-/Kleinschreibung) verwenden. Das Format ist üblicherweise „Benutzername@ISP“ anstelle von nur „Benutzername“.
Passwort	Geben Sie das Passwort ein. Sie können bis zu **128** alphanumerische Zeichen (Gross-/Kleinschreibung) verwenden.
Name des Dienstes	Dieses Element ist für Identifikationszwecke. Lassen Sie dieses Feld leer, sofern nichts anderes von Ihrem ISP angegeben ist. Die maximale Eingabelänge beträgt **15** alphanumerische Zeichen.
NAT	Die NAT (Network Address Translation) Funktion erlaubt es, mehreren Benutzern durch eine einzige IP Adresse den Zugriff aufs Internet zu ermöglichen. Wenn die Benutzer in Ihrem LAN eine öffentliche IP Adresse haben, können Sie die NAT Funktion deaktivieren.
IP (0.0.0.0:Auto)	Lassen Sie dieses Feld auf 0.0.0.0, um die IP Adresse automatisch von Ihrem ISP zu beziehen. Wenn Sie eine statische IP Adresse bei Ihrem ISP besitzen, tragen Sie diese in diesem Feld ein.
Authentifizierungs-Protokoll	Voreingestellt ist **Auto** und funktioniert mit den meisten ISPs. Gegebenenfalls gibt Ihr ISP Ihnen vor, ob Sie **Chap** oder **Pap** nutzen müssen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Verbindung	**Ständig verbunden:** Wenn Sie möchten, dass das Gerät eine PPPoE Verbindung beim Start aufbaut und auch bei einer Trennung durch den ISP automatisch wieder aufbaut, wählen Sie diese Einstellung. Wählen Sie diese auch, wenn Sie eine Flatrate Tarif besitzen. **Verbindung auf Anforderung:** Wenn Sie eine PPPoE Verbindung nur bei einem Zugriff zum Internet herstellen möchten (d.h. wenn ein Programm eines Computers eine Internetverbindung aufbaut), wählen Sie diese Einstellung.
Leerlaufzeit	Wenn für diese definierte Zeit keine Internetaktivität besteht, führt das Gerät eine automatische Trennung durch.
MTU	Maximum Transmission Unit ist die Grösse des grössten Datagramms (exkl. media-spezifische Header), das gesendet wird.
RIP	RIP v1, RIP v2 und RIP v2 Multicast. Wählen Sie die entsprechende Checkbox zur Aktivierung.
TCP MSS Clamp	Voreingestellt ist **Aktiviert**. Diese Option hilft Ihnen, die optimale Grösse der MTU automatisch festzustellen.
MAC Adressen Spoofing	Voreingestellt ist **Deaktiviert**. Diese Option wird von einigen Service Provider benötigt. Sie müssen die MAC Adresse, die Ihnen Ihr ISP vorgibt, eintragen.
Obtain DNS	Ein Domain Name System (DNS) enthält eine Mapping-Tabelle der Domänennamen und IP Adressen. DNS löst die IP Adressen für die spezifischen Domänennamen auf. Aktivieren Sie die Checkbox, um die DNS Server Adresse automatisch zu erhalten.
Primary	Geben Sie den primären DNS ein.
Secondary	Geben Sie den sekundären DNS ein.

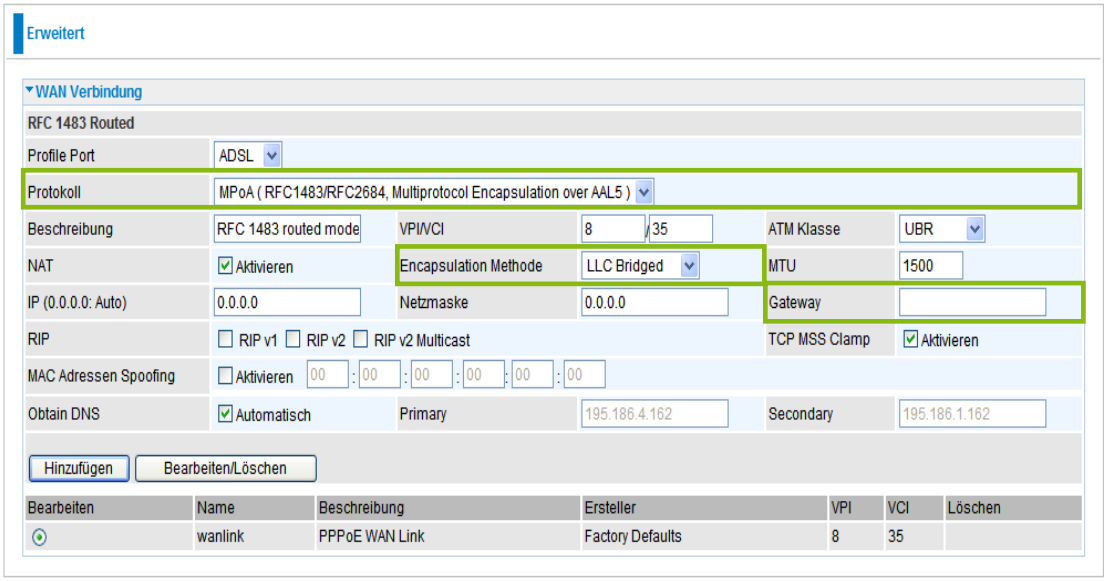
5.3.2.1.2. ADSL – PPPoA Verbindung

Für eine detaillierte Beschreibung der Parameter wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

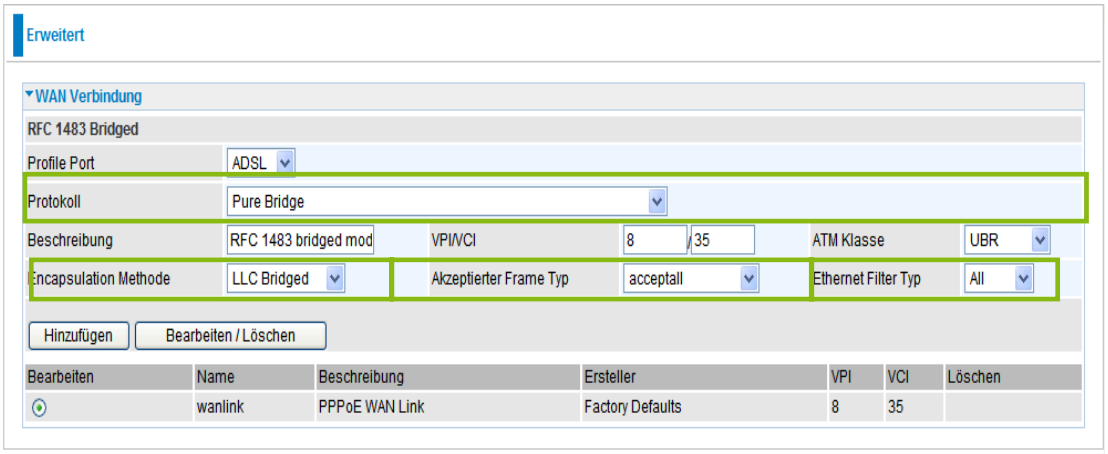
5.3.2.1.3. ADSL – MPoA Verbindung



Encap. Methode	Wählen Sie, ob Sie die Pakete an der WAN Schnittstelle als bridged oder routed Pakete haben möchten.
Gateway	Geben Sie die IP Adresse des Standard Gateways auf der WAN Seite an. Diese Einstellung ist obligatorisch, wenn die IP Adresse manuell gesetzt wird.

Für die anderen Einstellungen wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.

5.3.2.1.4. ADSL – Pure Bridge



Encap. Methode	Wählen Sie, ob Sie die Pakete an der WAN Schnittstelle als bridged oder routed Pakete haben möchten.
Akzeptierter Frame Typ	Geben Sie an, welcher Typ von Datenverkehr durch diese Verbindung geht: Alle Daten oder nur VLAN tagged.

© Internetagentur Schott GmbH, 2010. All rights reserved.

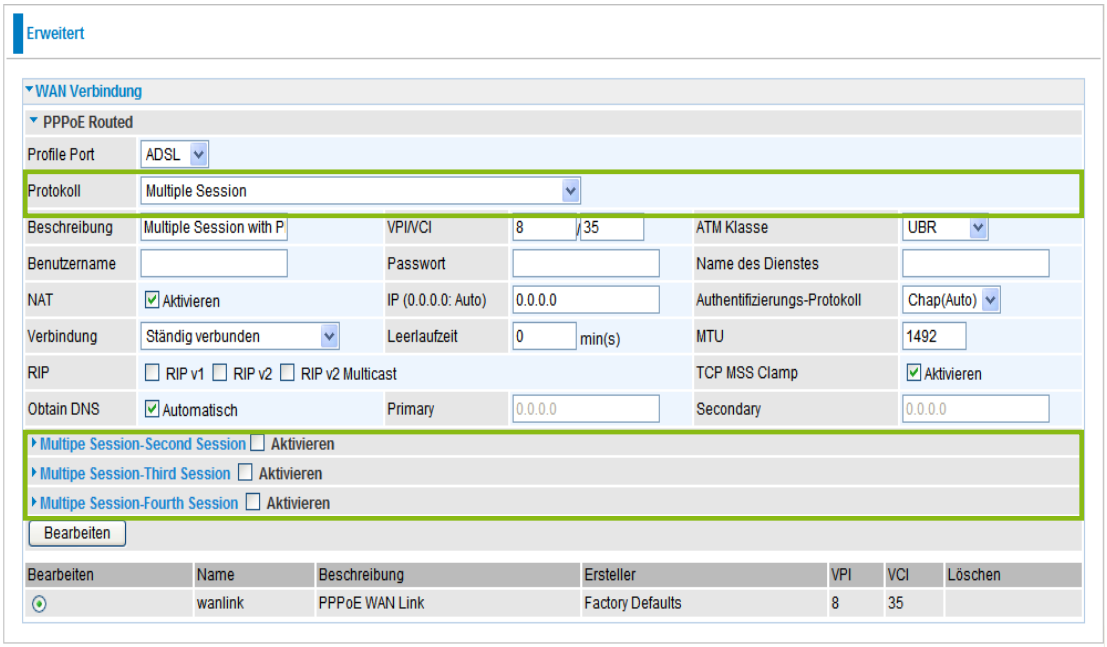
Ethernet Filter Typ	Geben Sie den von der genannten Bridge Schnittstelle ausgeführten Ethernet Filter Typ an.

All	Erlaubt alle Typen von Ethernet Paketen durch die Schnittstelle.
Ip	Erlaubt nur IP/ARP Typen von Ethernet Paketen durch die Schnittstelle.
PPPoE	Erlaubt nur PPPoE Typen von Ethernet Paketen durch die Schnittstelle.

Für die anderen Einstellungen wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.

5.3.2.1.5. ADSL – Multiple Session

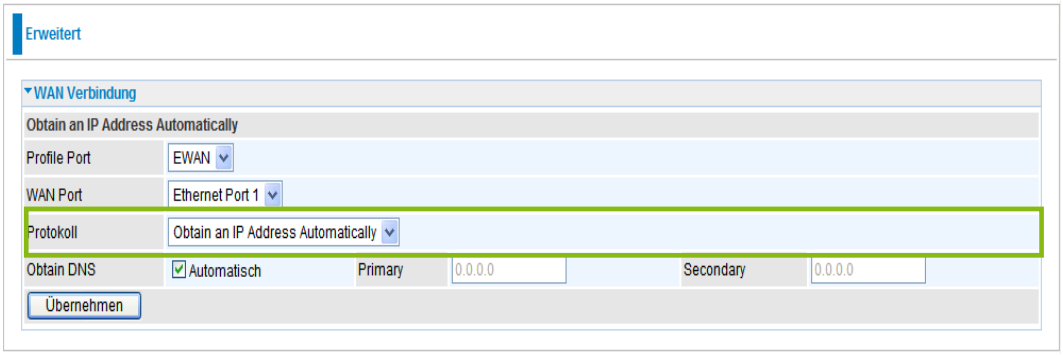
Diese Funktion erlaubt Ihnen, dass sich mehrere Benutzer über einen einzigen PVC authentifizieren können.
Für eine detaillierte Beschreibung der Parameter wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

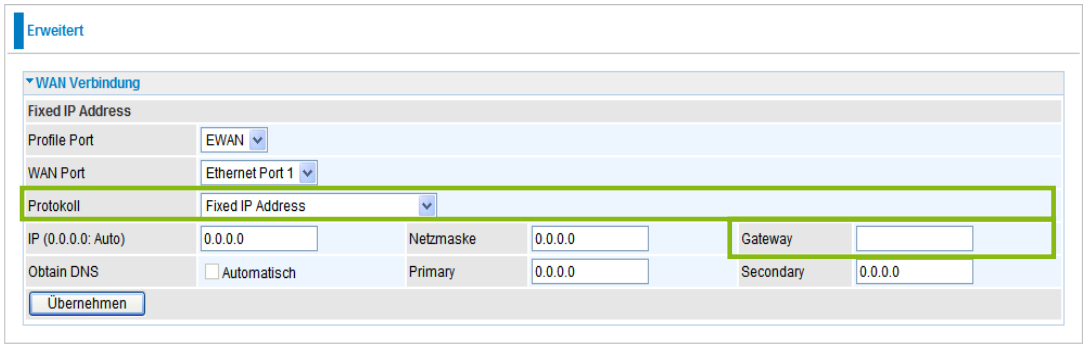
5.3.2.1.6. EWAN – Obtain IP Address Automatically → Für Internet via Satellit.

Dieses Verbindungsprotokoll wird für nicht-authentifizierte Verbindungen via Ethernet Anschluss 1 benutzt. Das Gerät benutzt DHCP um eine IP Adresse zu beziehen.
Für eine detaillierte Beschreibung der Parameter wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.



5.3.2.1.7. EWAN – Fixed IP Address → Für Internet via Satellit (z.B. satspeedPRO).

Dieses Verbindungsprotokoll wird für nicht-authentifizierte Verbindungen via Ethernet Anschluss 1 benutzt. Das Gerät benutzt eine statische IP Adresse.



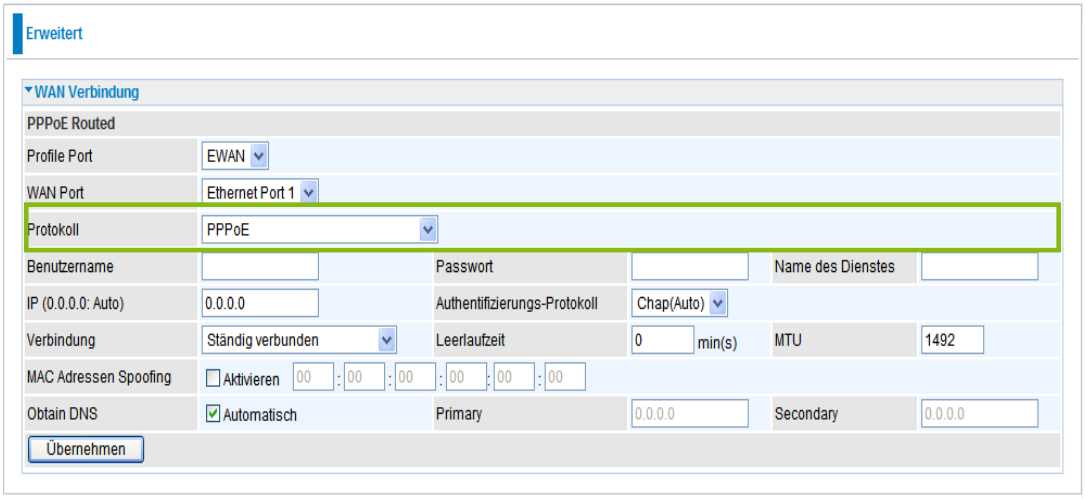
Gateway	Geben Sie die IP Adresse des Standard Gateways auf der WAN Seite an. Diese Einstellung ist obligatorisch, wenn die IP Adresse manuell gesetzt wird.

Für die anderen Einstellungen wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

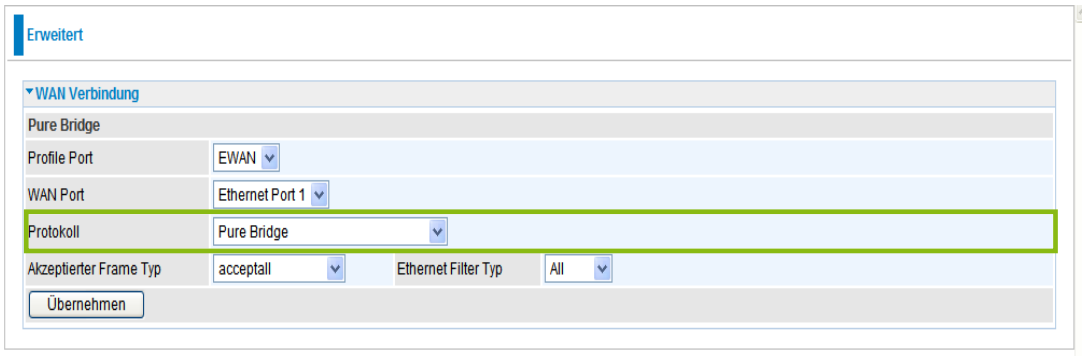
5.3.2.1.8. EWAN – PPPoE

Dieses Verbindungsprotokoll wird für authentifizierte Verbindungen via Ethernet Anschluss 1 benutzt.
Für eine detaillierte Beschreibung der Parameter wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.



5.3.2.1.9. EWAN – Pure Bridge

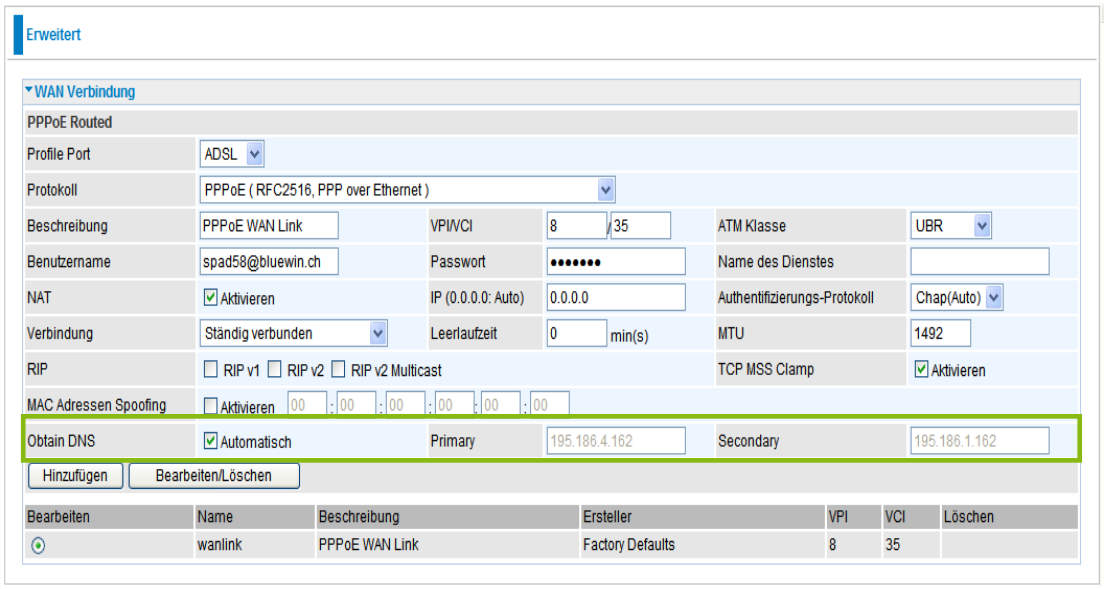
Dieses Verbindungsprotokoll wird für Eins-zu-Eins Verbindungen via Ethernet Anschluss 1 benutzt.
Für eine detaillierte Beschreibung der Parameter wird auf Kapitel **5.3.2.1.1 ADSL – PPPoE Verbindung** verwiesen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

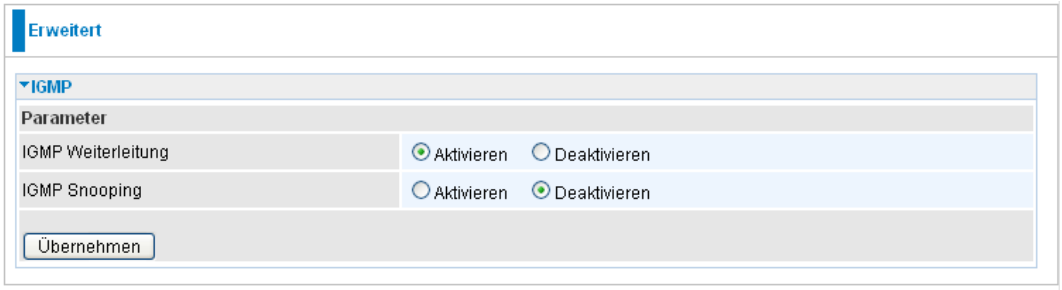
5.3.2.2 DNS Server

Voreingestellt ist **Automatisch**. Diese Einstellung erlaubt es Ihnen, den primären und sekundären DNS Server pro WAN Verbindung zu ändern.



5.3.2.3 IGMP Proxy (Experten)

IGMP, bekannt als *Internet Group Management Protocol*, wird gebraucht, um Hosts aus Multicast Gruppen zu verwalten.

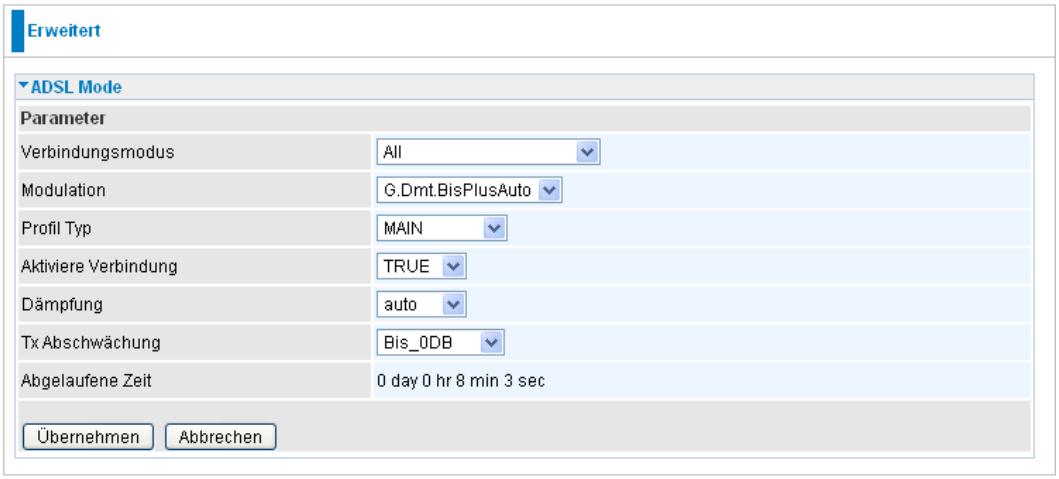


IGMP Weiterleitung	Voreingestellt ist **Aktiviert**. Akzeptiert Multicast Pakete.
IGMP Snooping	Voreingestellt ist **Deaktiviert**. Erlaubt dem Ethernet Überprüfungen durchzuführen und korrekte Entscheidungen bezüglich der Weiterleitung der Pakete zu treffen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.2.4 ADSL (Experten)

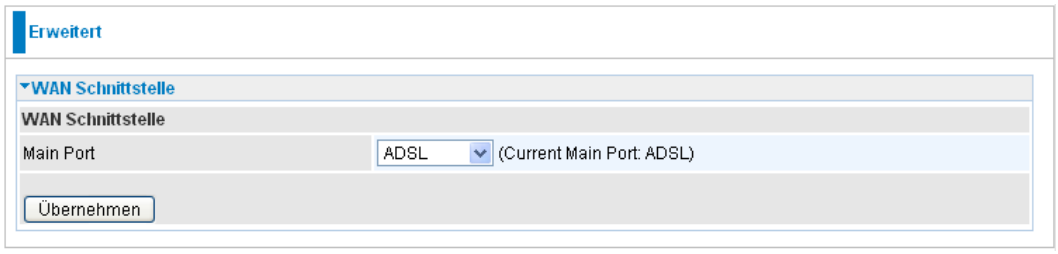
Diese Einstellungen betreffen Ihre ADSL Verbindung. Ändern Sie diese nicht, ausser Ihr ISP gibt Ihnen das vor.



Verbindungsmodus	Diese Einstellung erlaubt Ihnen, den ADSL Modus manuell zu ändern. Sie können aus verschiedenen ADSL Verbindungsmodi wählen: All, AnnexM2+, AnnexM2, ADSL, ADSL 2+ und ADSL 2.
Modulation	Dieser Eintrag ist nicht änderbar. Das Gerät erkennt automatisch die Eigenschaften Ihrer ADSL Verbindung.
Profil Typ	Zeigt voreingestellte ISP Einstellungen.
Aktiviere Verbindung	Hier können Sie die Verbindung aktivieren und deaktivieren.
Dämpfung	Diese Funktion reduziert die Sendeleistung des Gerätes, was dessen Downstream Performance beeinflusst. Höhere Sendeleistung kann die Downstream Performance erhöhen, jedoch zu einer instabilen ADSL Verbindung führen.
Abgelaufene Zeit	Zeigt die Zeit seit der letzten ADSL Synchronisation.

5.3.2.5 WAN Schnittstelle (Experten)

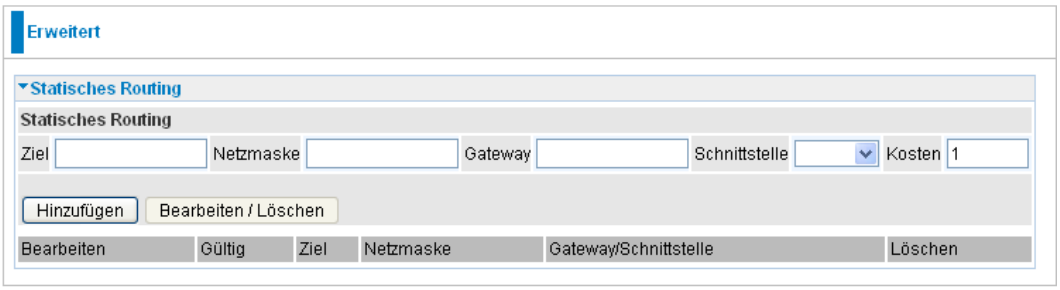
Hier können Sie Ihre WAN Verbindung konfigurieren
Treffen Sie eine Auswahl für den **Main Port** (ADSL oder EWAN) und klicken Sie auf **Übernehmen**.



© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.3. IP Routing (Experten)

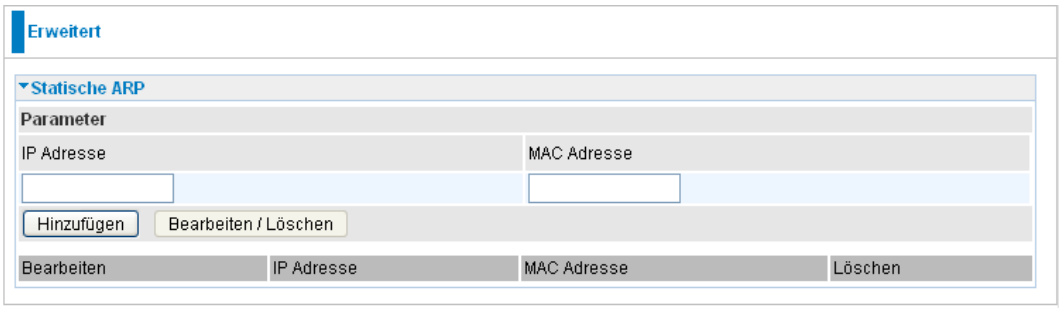
5.3.3.1 Statisches Routing



Ziel	Geben Sie die Zielsubnetz IP Adresse ein.
Netzmaske	Geben Sie die Subnetzmaske der Ziel IP Adresse, basiert auf der oberen Zeile, ein.
Gateway	Geben Sie die Gateway IP Adresse ein, an welche die Pakete weitergeleitet werden sollen.
Schnittstelle	Geben Sie die Schnittstelle an, durch welche die Pakete weitergeleitet werden sollen.
Kosten	Geben Sie die Anzahl Hops an, um die Zieladresse mittels dieser Route zu erreichen.

5.3.3.2 Statische ARP

Diese Seite erlaubt Ihnen, IP Adressen spezifische MAC Adressen statisch zuzuordnen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

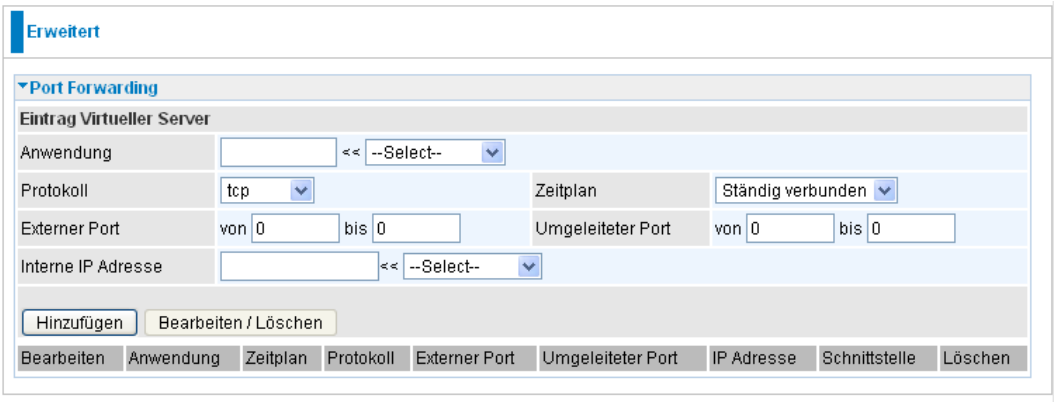
5.3.4. Virtuelle Server

5.3.4.1 Port Forwarding

Ein Port ist eine Nummer (zwischen 0 und 65535), welche von einer/m Applikation/Programm benutzt wird. Einige Ports sind vordefiniert (0-1000) und bekannt als „well-known Ports“. Server folgen den well-known Port Zuordnungen, sodass Clients diese lokalisieren können.
Wenn Sie einen Server in Ihrem Netzwerk betreiben und wünschen, dass dieser vom WAN aus erreicht werden kann, benötigen Sie Port Forwarding. Beispiel dafür sind Applikation, die eingehende Verbindungen (z.B. Peer-to-Peer (P2P) Software wie Instant Message und File-Sharing Applikationen; Online Game Host Server) in Ihrem Netzwerk benötigen. Damit die eingehenden Verbindungsversuche von Ihrem Gerät zugelassen werden, müssen Sie die benötigten Ports frei schalten.
Der Grund ist, dass bei Verwendung von NAT, Ihre öffentliche IP Adresse verwendet wird. Folglich müssen Sie einen öffentlichen Port einer IP Adresse in Ihrem lokalen Netzwerk zuweisen. Das Gerät kann als virtueller Server eingerichtet werden, sodass entfernte Benutzer, die auf Services wie Web oder FTP via einer öffentlichen (WAN) IP Adresse zugreifen, automatisch an einen lokalen Server im LAN umgeleitet werden können. Je nach angefordertem Service (TCP/UDP, Port Nummer), leitet das Gerät die externe Anfrage an den entsprechenden Server im lokalen Netzwerk weiter.

Einen virtuellen Server hinzufügen

Weil NAT als „natürliche“ Internet Firewall agiert, schützt Sie Ihr Gerät von Zugriffen aus dem Internet, indem alle eingehenden Verbindungen nur bis zu Ihrem Gerät gelangen, sofern Sie keinen virtuelle Server eingerichtet haben, der die Ports zu Ihren lokalen Rechnern im Netzwerk weiterleitet.
Wenn Ihr Gerät Zugriff auf interne Server erlauben soll – z.B. einen Web Server, FTP Server, Email Server oder Game Server – dann agiert es als ein „virtueller Server“. Sie können einen lokalen Server mit einer spezifischen Port Nummer aufsetzen, z.B. web/HTTP (Port 80), FTP (Port 21), Telnet (Port 23), SMTP (Port 25) oder POP3 (Port 110). Wenn das Gerät einen eingehenden Verbindungsversuch für einen spezifischen Port erhält, dann wird dieser zum angegebenen internen Server weitergeleitet.



Anwendung	Geben Sie hier eine eigene Beschreibung ein, um diesen Eintrag zu identifizieren oder wählen Sie eine bereits bestehende Anwendung aus dem Pull Down Menu aus.
--Select-- **Pull Down Menü**	20 vordefinierte Anwendungen sind verfügbar. Anwendung, Protokoll und Externer/Umgeleiteter Port werden automatisch ausgefüllt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

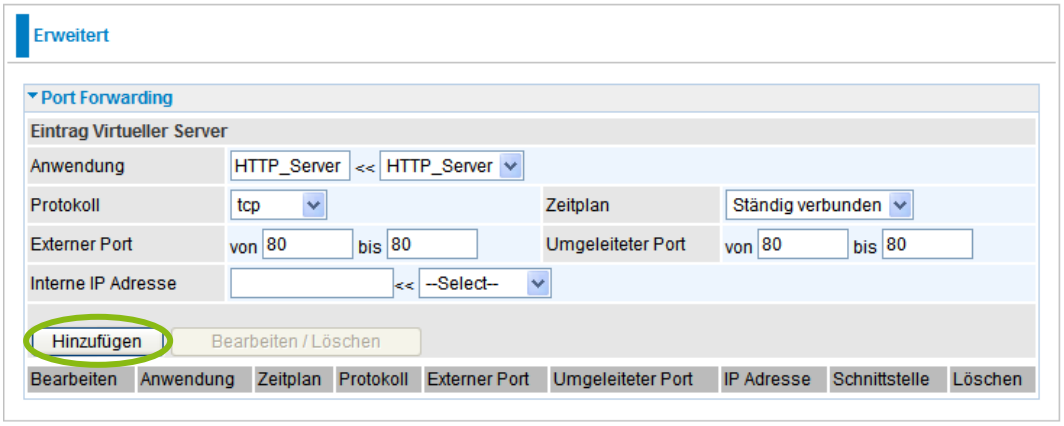
Protokoll	Unterstütztes Protokoll für den virtuellen Server. Zusätzlich zur Port Nummer, müssen Sie das benutzte Protokoll angeben. Dieses wird durch die Anwendung vorgegeben, die meisten Anwendungen benutzen TCP oder UDP.
Zeitplan	Benutzerdefinierte Zeitspanne, während der der virtuelle Server aktiviert ist. Sie können einen Zeitplan oder „Ständig Verbunden“ angeben. Für detaillierte Informationen wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
Externer Port	Port Nummer, auf der WAN Seite des Gerätes, die bei einem Zugriff auf Ihren virtuellen Server benutzt wird.
Umgeleiteter Port	Port Nummer, die vom lokalen Server im LAN Netzwerk benutzt wird.
Interne IP Adresse	Die private IP Adresse im lokalen Netzwerk, mit welcher der virtuelle Server betrieben wird. Das Pull Down Menü listet alle bestehenden verbundenen Netzwerk Clients auf.

Um einen neuen Eintrag hinzuzufügen, füllen Sie die angeforderten Informationen aus und klicken Sie auf **Hinzufügen**.
Um Einstellungen eines bestehenden Eintrages zu ändern, wählen Sie den **Bearbeiten** Radio Button, führen Sie Ihre Änderungen durch und klicken Sie auf **Bearbeiten/Löschen**.
Um einen Eintrag zu löschen, wählen Sie den **Löschen** Radio Button und klicken Sie auf **Bearbeiten/Löschen**.

Beispiel

Wenn Sie einen WEB Server in Ihrem lokalen Netzwerk betreiben und Sie diesen im Internet zugänglich machen wollen, müssen Sie Port Nummer 80 (Web/HTTP) aktivieren und diesen auf die IP Adresse des Servers leiten. Alle eingehenden HTTP Anfragen aus dem Internet werden nun zur IP Adresse des Servers weitergeleitet.

Beispieldaten:
Anwendung: *HTTP_Sever*
Zeitplan: *Ständig verbunden*
Protokoll: *tcp*
Externer Port: *80-80*
Umgeleiteter Port: *80-80*
IP Adresse: *192.168.100.2*



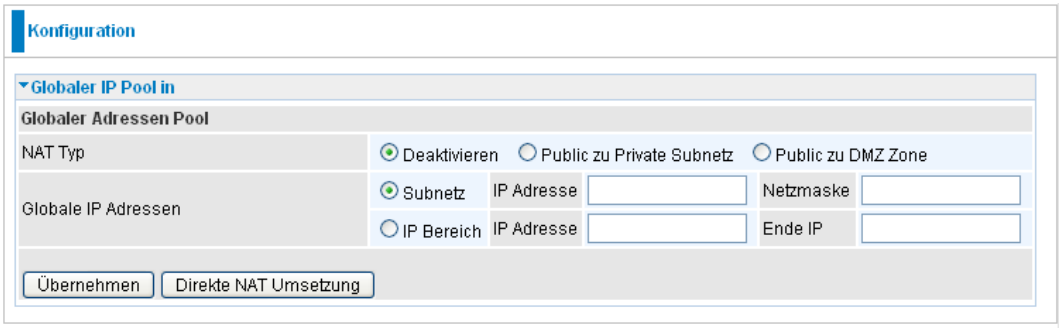
© Internetagentur Schott GmbH, 2010. All rights reserved.

Bemerkung	**Wenn Sie Port Forwarding benutzen, kann das Einfluss auf die Sicherheit haben, da Benutzer von ausserhalb auf Ihre sich im LAN befindlichen Rechner zugreifen können. Deshalb wird empfohlen, dass Sie nur die spezifischen Ports öffnen, die Ihre Anwendungen benötigen.**
Warnung	**Wenn Sie NAT deaktiviert haben, wird die virtuelle Server Funktion nicht funktionieren.** **Wenn Sie die DHCP Server Option aktiviert haben, müssen Sie bedenken, dass sich die IP Adressen im lokalen Netzwerk dynamisch ändern können. Um dies zu vermeiden, weisen Sie Ihren Servern statische IP Adressen zu. Für eine detaillierte Erklärung wird auf Kapitel 5.3.1.2 DHCP Server verwiesen.**

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.4.2 Direkte NAT Umsetzung (Experten)

Direkte NAT Umsetzung erlaubt es Ihnen, den Clients in Ihrem lokalen Netzwerk mehrere WAN IP Adressen zuzuweisen.



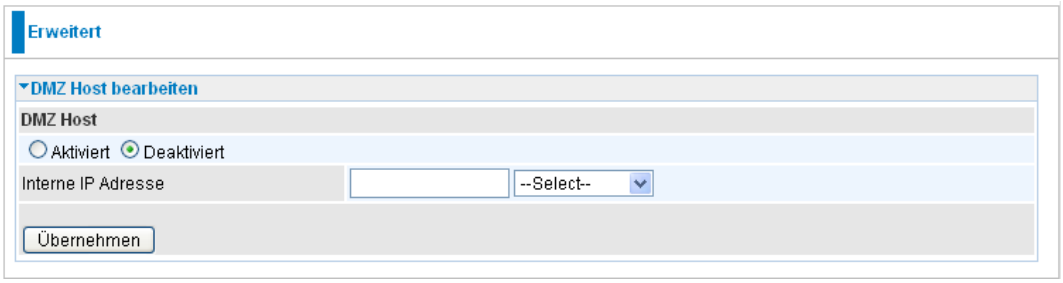
5.3.4.3 UPnP Regeln

Diese Seite listet alle Port-Mappings, die UPnP (Universal Plug and Play) benutzen, auf. Dies ist eine schreibgeschützte Seite, welche nur zur Information dient.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.4.4 DMZ Host

Der DMZ Host ist ein lokaler Computer, welcher jederzeit vom Internet kontaktiert werden kann. Wenn Sie eine interne IP Adresse als DMZ Host konfigurieren, werden alle ankommenden Pakete zu diesem DMZ Host geleitet, sofern das Paket nicht eine Port Nummer benutzt, die bereits von einem anderen virtuellen Server genutzt wird.



DMZ Host	Voreingestellt ist **Deaktiviert**. **Aktiviert:** Aktiviert die DMZ Funktion. **Deaktiviert:** Deaktiviert die DMZ Funktion.
Interne IP Adresse	Ist der **Aktiviert** Radio Button gewählt, müssen Sie dem DMZ Host eine statische IP Adresse zuweisen. Seien Sie sich bewusst, dass diese IP Adresse im WAN/Internet zugänglich ist.
--Select-- **Pull Down Menü**	Listet alle Clients, die mit dem lokalen Netzwerk verbunden sind, auf.

Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

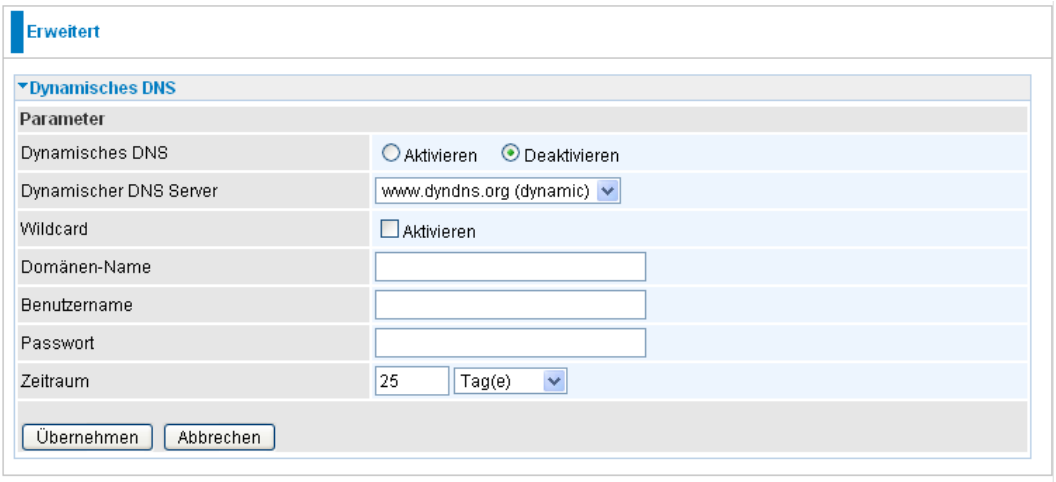
Für detaillierte Informationen zur Zuweisung einer statischen IP Adresse wird auf Kapitel **5.3.1.2 DHCP Server** verwiesen.

5.3.4.5 Dynamisches DNS

Die Dynamische DNS Funktion erlaubt Ihnen, dynamischen (d.h. sich periodisch ändernden) IP Adressen (z.B. die WAN IP Adresse des Geräts) einen statischen Hostnamen zuzuweisen. Damit ermöglicht es Benutzern, die von ihrem ISP keine statische IP Adresse erhalten, einen Domänennamen zu benutzen. Dies ist sehr hilfreich, um einen Server via ADSL Leitung zu betreiben, auf den man dann von ausserhalb über einen Domänennamen zugreifen kann, statt über eine sich dynamisch ändernden IP Adresse.

Dazu müssen Sie sich aber zuerst bei einem Dynamic DNS Provider registrieren, beispielsweise: www.dyndns.org

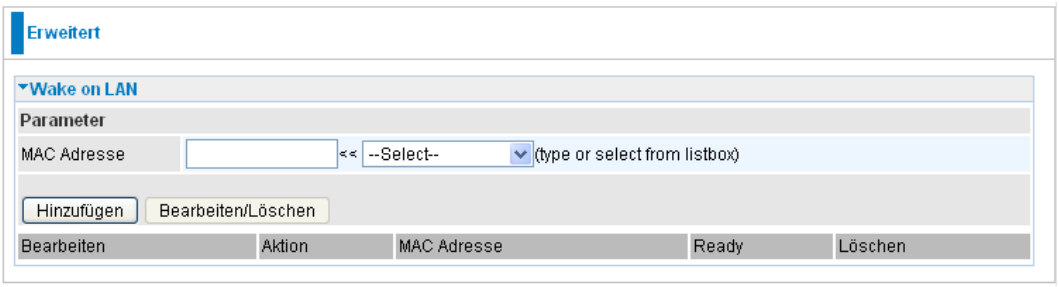
© Internetagentur Schott GmbH, 2010. All rights reserved.

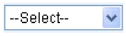


Dynamisches DNS	Voreingestellt ist **Deaktiviert**. **Deaktiviert:** Deaktiviert die DDNS Funktion. **Aktiviert:** Aktiviert die DDNS Funktion.
Dynamischer DNS Server	Wählen Sie den DDNS Service, bei dem Sie ein Konto registriert haben.
Domänen-Name **Benutzername** **Passwort**	Geben Sie Ihren registrierten Domänenname, Ihren Benutzernamen und Ihr Passwort für diesen Service ein.
Zeitraum	Gibt die Zeitspanne für den Austausch von Informationen zwischen dem Gerät und dem DDNS Server an. Zusätzlich dazu, wird das Gerät, bei einer Änderung Ihrer dynamischen IP Adresse, ein Update durchführen.

5.3.4.6 Wake on LAN

Wake on LAN erlaubt Ihnen, einen Computer remote zu starten. Diese Funktion kann nur genutzt werden, wenn Wake on LAN (WoL) von Ihrer Computerhardware unterstützt wird.



Wählen Sie eine MAC Adresse mittels dem 

Pull Down Menü aus oder geben Sie manuell eine MAC Adresse ein. Bestätigen Sie die Eingabe, indem Sie auf **Hinzufügen** klicken.
Sobald eine MAC Adresse eingegeben ist, klicken Sie den Button in der Aktion Spalte, um den Computer zu starten.

© Internetagentur Schott GmbH, 2010. All rights reserved.

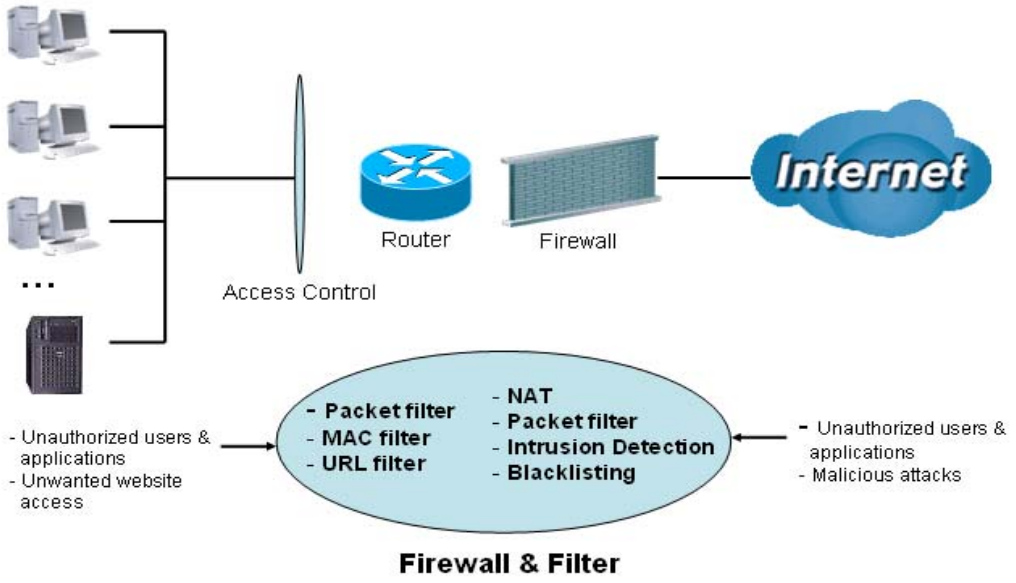
5.3.5. NAT ALG (Experten)

SIP ALG	Voreingestellt ist **Aktiviert**. Dies stellt eine ordnungsgemässe Funktionalität der SIP Clients im lokalen Netzwerk sicher.
FTP ALG	Voreingestellt ist **Aktiviert**. Dies stellt eine ordnungsgemässe Funktionalität der FTP Clients im lokalen Netzwerk sicher.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.6. Firewall (Experten)

Ihr Gerät enthält eine SPI (Stateful Packet Inspection) Firewall, um den Internet Zugriff Ihres LANs zu kontrollieren sowie Angriffe von Hackern zu verhindern. Bei Benutzung von NAT, agiert das Gerät als „natürliche“ Internet Firewall, weil alle Computer in Ihrem LAN private IP Adressen benutzen, die nicht vom Internet erreichbar sind.

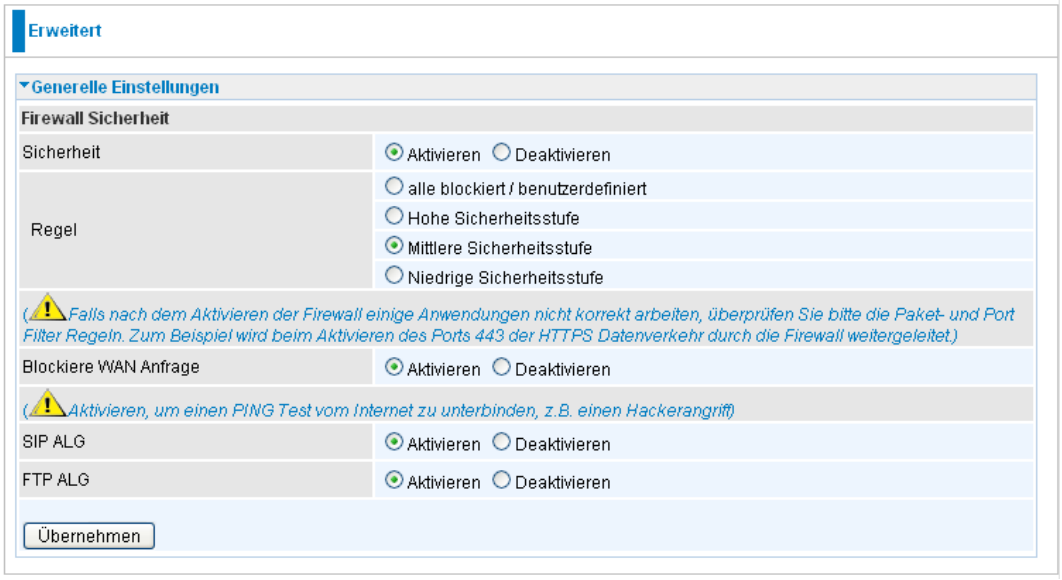


Firewall & Filter

Bemerkung	**Wenn Sie virtuelle Server benutzen, wird Ihr PC in soweit dem Internet zugänglich sein, wie Sie das in den Regeln definiert haben.**

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.6.1 Allgemein



Sicherheit	Voreingestellt ist **Aktiviert**. **Aktiviert:** Aktiviert die Firewall Funktion. **Deaktiviert:** Deaktiviert die Firewall Funktion.
Regel	Es gibt vier Optionen, wenn Sie die Firewall aktivieren: **alle blockiert/benutzerdefiniert**: Es gibt keine voreingestellten Port- oder Adressfilterregeln, d.h., dass alle ankommenden (Internet zu LAN) und ausgehenden (LAN zu Internet) Pakete blockiert werden. Sie müssen Ihre eigenen Filterregeln für den Zugriff zum Internet hinzufügen. Wählen Sie entweder **Hohe, Mittlere** oder **Niedrige Sicherheitsstufe**, um die Firewall mit den vordefinierten Regeln zu aktivieren. Für detaillierte Informationen wird auf Tabelle **Tabelle 1 Firewall Levels** verwiesen.
Blockiere WAN Anfrage	Dies ist eine eigenständige Funktion und steht nicht in Verbindung mit den Sicherheitseinstellungen. Meistens wird Sie gebraucht, um Scan-Tools vom WAN, welche von Hackern gebraucht werden, abzuwehren.

Wählen Sie **Übernehmen**, um die Änderungen zu speichern.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Anwendung	Protokoll	Port Nummer	Firewall Regel		
			Niedrig	Mittel	Hoch
PING	ICMP		→	→	→
HTTP (Web server)	TCP	80	→	→	→
DNS	TCP/UDP	53	→	→	→
SMTP (Sending Mails)	TCP	25	→	→	→
POP3 (Receiving Mails)	TCP	110	→	→	→
RealAudio / RealVideo	UDP	7070	↔	↔	
H.323	TCP	1720	↔	→	
T.120	TCP	1503	↔	→	
FTP	TCP	21	→	→	
Telnet	TCP	23	→	→	
News (NNTP)	TCP	119	→	→	
SSH	TCP	22	→	→	
NTP / SNTP	UDP	123	→	→	
HTTPS	TCP	443	→	→	
ICQ	TCP	5190	↔		
MSN	TCP	1863	↔		
MSN	UDP	7001	↔		
MSN Video	TCP	9000	→		
HTTP Proxy	TCP	8080	→		

Tabelle 1 Firewall Levels

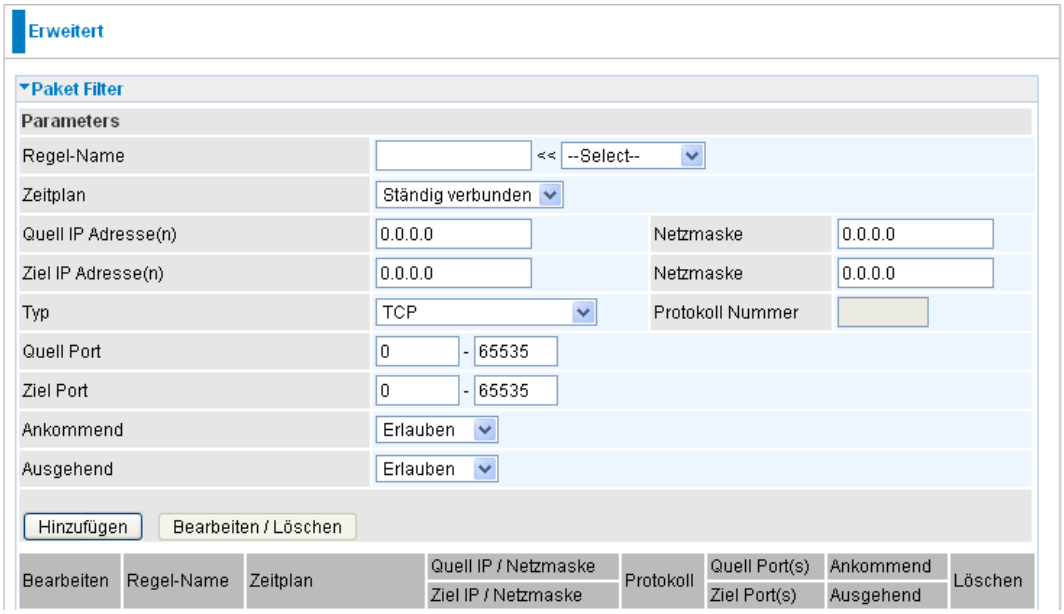
↔	Ankommende und ausgehende Verbindungen werden erlaubt.
→	Ausgehende Verbindungen werden erlaubt.
←	Ankommende Verbindungen werden erlaubt.
	Keine Verbindungen werden erlaubt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.6.2 IP Filter

Diese Funktion ist nur verfügbar, wenn die Firewall eingeschaltet ist und eine Regel gewählt ist (Alle blockieren, Hohe, Mittlere oder Niedrige Sicherheitsstufe). Die voreingestellten Portfilterregeln im Paketfilter müssen entsprechend den Firewall Regeln angepasst werden. Sehen Sie dazu die Erläuterungen in der **Tabelle 1 Firewall Levels**.

Eine neue Regel hinzufügen



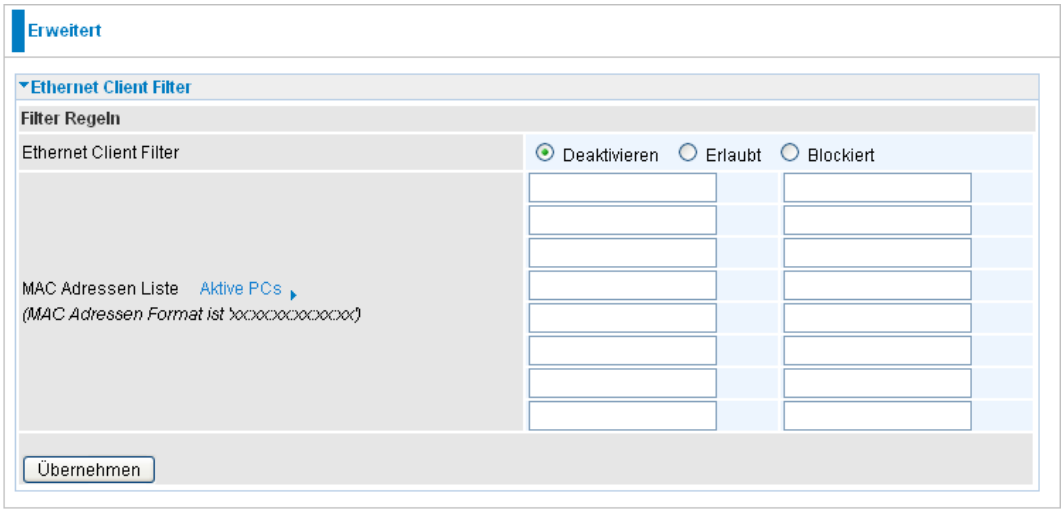
Regel-Name	Geben Sie einen Namen ein, um diesen Eintrag zu definieren oder klicken Sie auf das **'Select'** Pull Down Menü, um eine vordefinierte Regel auszuwählen. Die maximale Länge des Namens beträgt 32 Zeichen.
Zeitplan	Benutzerdefinierter Zeitschlitz oder Ständig verbunden. Für nähere Informationen wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
Quell IP Adresse(n) / Ziel IP Adresse(n)	Dies beschreibt den IP Adressfilter, um Verkehr von/zu einzelnen IP Adresse(n) zu erlauben/ blockieren. **Tipp:** Um Zugriff zu/von einer einzelnen IP Adresse zu blockieren, geben Sie die IP Adresse als **Host IP Adresse** ein und benutzen Sie eine **Netmaske** von "255.255.255.255".
Typ	Dies beschreibt den Paketprotokolltyp, der von der Anwendung benutzt wird. Sie können zwischen **TCP**, **UDP** oder beidem **TCP/UDP** wählen. Sie können im Feld rechts auch ein anderes Protokoll angeben.
Protokoll Nummer	Geben Sie die Nummer des spezifizierten Protokolls ein.
Quell Port	Der Port oder Portbereich, der von der Remote Seite/ WAN für eine Verbindung auf die Anwendung genutzt werden darf. Voreingestellt ist der Bereich **0 - 65535**.
Ziel Port	Der Port oder Portbereich, der die Anwendung definiert.
Ankommend / Ausgehend	**Erlauben** oder **Blockieren** Sie den Zugriff auf (**„ausgehend"**) oder von (**„ankommend"**) das/dem Internet.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Um einen neuen Eintrag hinzuzufügen, füllen Sie die benötigten Informationen aus und klicken Sie auf **Hinzufügen**.
Um bereits bestehende Einträge zu ändern, wählen Sie den **Bearbeiten** Radio Button, machen Sie Ihre Änderungen und klicken Sie auf **Bearbeiten/Löschen**.
Um einen Eintrag zu löschen, wählen Sie den **Löschen** Radio Button und klicken Sie auf **Bearbeiten/Löschen**.

5.3.6.3 MAC Filtering

Die Zugangskontrolle (MAC Filter) unterstützt bis zu 16 Ethernet Netzwerk Clients und erlaubt entweder Datenverkehr von autorisierten Clients anzunehmen oder von ungewünschten Clients abzublocken.
Es sind keine voreingestellten MAC Adressen-Filterregel.



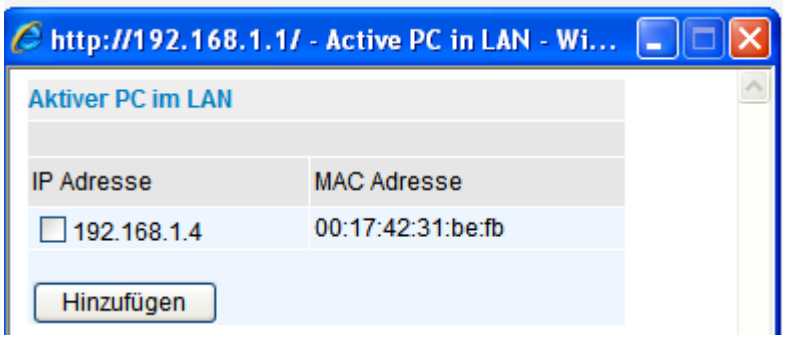
Ethernet Client Filter	Voreingestellt ist **Deaktivert**.
	Erlaubt: Klicken Sie diesen Radio Button, um Clients den Zugriff auf Ihr lokales Netzwerk zu erlauben, indem Sie deren MAC Adressen in die Zeilen eintragen. Oder klicken Sie Aktive PCs, um eine Liste der aktuell verbundnen Clients anzuzeigen. Stellen Sie sicher, dass MAC Adressen Ihrer PCs aufgelistet sind.
	Blockiert: Klicken Sie diesen Radio Button, um unerwünschten Zugriff von Clients auf Ihr lokales Netzwerk zu verbieten, indem Sie deren MAC Adressen in die Zeilen eintragen. Oder klicken Sie Aktive PCs, um eine Liste der aktuell verbundnen Clients anzuzeigen. Stellen Sie sicher, dass MAC Adressen Ihrer PCs **nicht** aufgelistet sind.
Aktive PCs Aktive PCs	Hier werden die Clients, die mit Ihrem Gerät per Ethernet-Ports verbunden sind, aufgelistet. Nähere Informationen dazu finden Sie im Kapitel Aktive PCs – Aktiver PC in LAN**5.3.6.3.1 Aktive PCs – Aktiver PC in LAN**

Die maximale Anzahl Clients beträgt 16. Die MAC Adressen sind 6 Bytes lang; sie bestehen nur aus hexadezimalen Zeichen. Die Ziffern 0-9 und a-f werden somit akzeptiert.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Bemerkung: Befolgen Sie das übliche Format von MAC-Adressen xx:xx:xx:xx:xx:xx. Der Doppelpunkt (:) ist Teil dieses Formates.

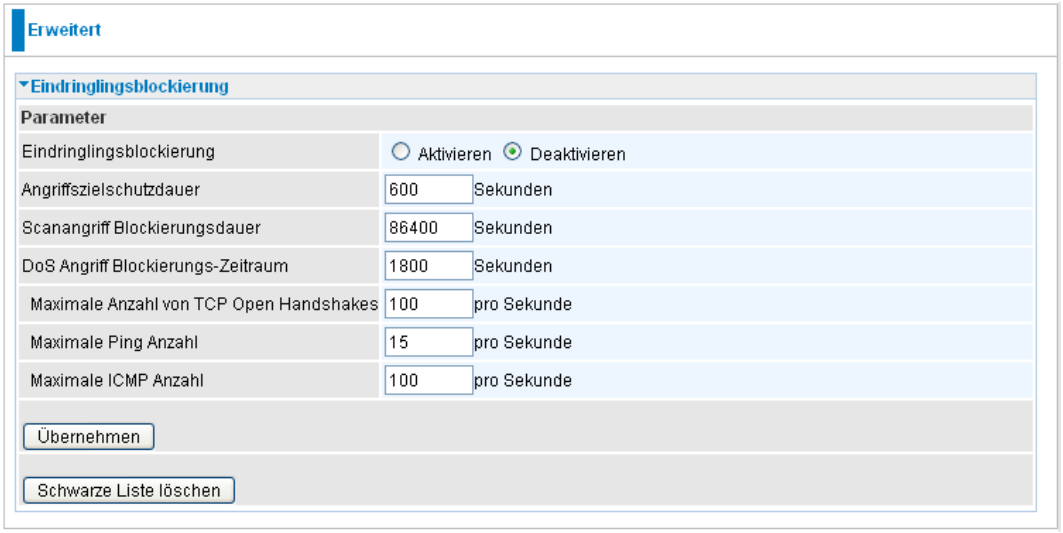
5.3.6.3.1. Aktive PCs – Aktiver PC in LAN



Aktiver PC im LAN ist eine Liste der MAC Adressen der mit dem Gerät verbundenen Netzwerkclients.
Klicken Sie die Checkbox eines aufgelisteten Clients an, und danach auf **Hinzufügen**, um den Client in die MAC Adressliste aufzunehmen.

5.3.6.4 Eindringlingsblockierung

Die Eindringlingsblockierung des Geräts (IDS, Intrusion Dection System) erkennt Hackerangriffe und Eindringversuche aus dem Internet. Wenn die IDS Funktion der Firewall eingeschaltet ist, werden ankommende Pakete gefiltert und blockiert, wenn Sie als möglicher Hackerangriff, Eindringlingsversuch oder andere suspekte Verbindung erkannt werden.



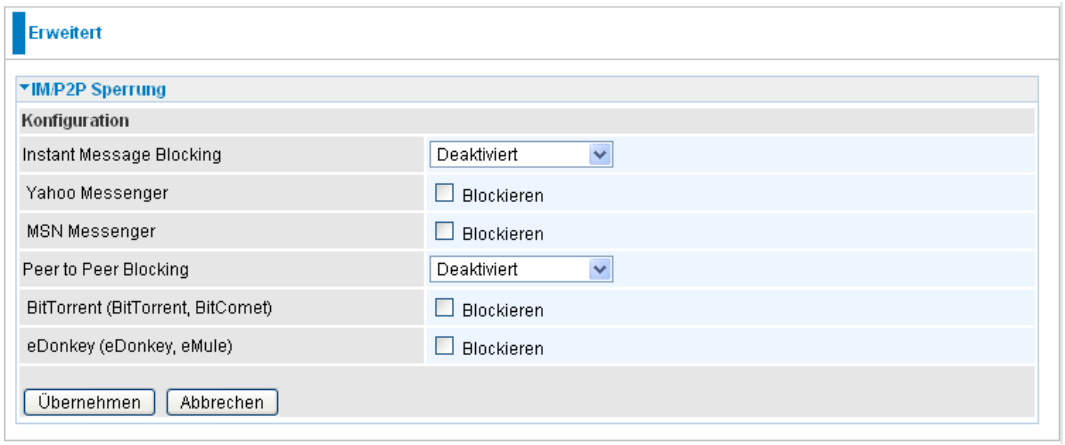
Eindringlings-blockierung	Voreingestellt ist **Deaktiviert**. Aktivieren Sie IDS, um böswillige Attacken zu erkennen, verhindern und zu loggen. Wenn die Funktion eingeschaltet ist, wird sie Smurf Angriffe blockieren.
Blockierungs-dauer	**Angriffszielschutz:** Dies ist die Zeitspanne für das Blockieren der Smurf Angriffe. Voreingestellt sind 600 Sekunden.

© Internetagentur Schott GmbH, 2010. All rights reserved.

	Scanangriff: Dies ist die Zeitspanne für das Blockieren der Hosts, die einen möglichen Scanangriff zu unternehmen versuchen. Scan Angriffstypen enthalten *X'mas scan, IMAP SYN/FIN scan* und ähnliche Versuche. Voreingestellt sind 86400 Sekunden.
	DoS Angriff: Dies ist die Zeitspanne für das Blockieren der Hosts, die einen möglichen DoS Angriff zu unternehmen versuchen. Voreingestellt sind 1800 Sekunden
Maximale Anzahl von TCP Open Handshakes	Dies ist ein Schwellwert, bei welchen entschieden wird, ob ein *SYN Flood* Versuch vorliegt oder nicht. Voreingestellt sind 100 TCP SYN pro Sekunde.
Maximale PING Anzahl	Dies ist ein Schwellwert, bei welchen entschieden wird, ob ein *ICMP Echo Storm* Versuch vorliegt oder nicht. Voreingestellt sind 15 ICMP Echo Requests (PING) pro Sekunde.
Maximale ICMP Anzahl	Dies ist ein Schwellwert, bei welchen entschieden wird, ob ein *ICMP flood* Versuch vorliegt oder nicht. Voreingestellt sind 100 ICMP Pakete pro Sekunde, ICMP Echo Requests (PING) ausgeschlossen. Für *SYN Flood*, *ICMP Echo Storm* und *ICMP flood*, wird IDS den User im Event Log nur warnen. IDS kann Sie nicht gegen solche Angriffe schützen.
Schwarze Liste löschen	Wenn das Gerät einen möglichen Angriff entdeckt, wird die Quell IP Adresse oder Ziel IP Adresse zur schwarzen Liste hinzugefügt. Jeder künftige Angriff, der diese IP Adresse benutzt, wird während der in der **Blockierungsdauer** angegebenen Zeit blockiert. Die schwarze Liste ist nicht sichtbar und kann nur gelöscht werden.

5.3.6.5 Instant Messaging (IM) / Peer to Peer (P2P) Sperrung

IM benötigt eine Client Programm Software, die es Benutzern erlaubt, Textmeldungen mit anderen IM Benutzern via Internet in Echtzeit auszutauschen.
P2P Anwendungen benutzen eine Gruppe von Benutzern, die Dateien durchs Internet austauschen.
Beide, IM und P2P Anwendungen, machen die Kommunikation schneller und einfacher, aber Ihr Netzwerk dadurch auch unsicherer. Die IM und P2P Sperrung des Gerätes hilft Ihnen, LAN Computern die Benutzung der meist benutzten IM Anwendungen, Yahoo und MSN und P2P Anwendungen, BitTorrent und eDonkey über das Internet zu verbieten.

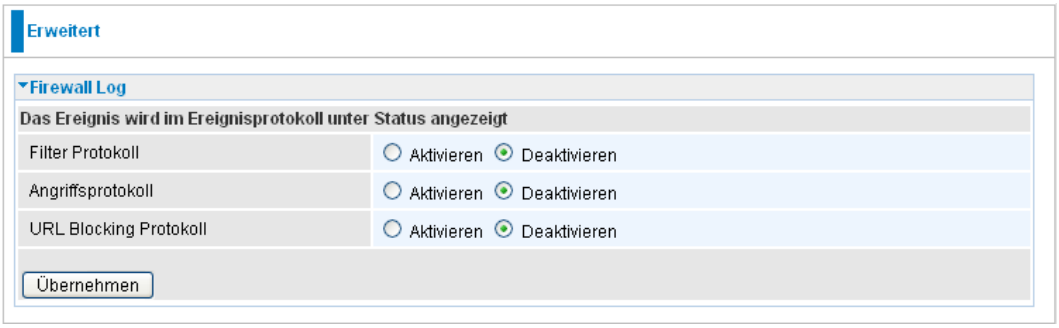


© Internetagentur Schott GmbH, 2010. All rights reserved.

Instant Message Blocking	Voreingestellt ist **Deaktiviert**. **Deaktiviert:** Die Instant Message Sperrung ist deaktiviert. **Ständig verbunden:** Die IM Sperrung ist aktiviert. **TimeSlot1 ~ TimeSlot16:** Dies ist der benutzerdefinierte Zeitschlitz. Für eine detaillierte Beschreibung wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
Yahoo/MSN Messenger	Stellen Sie zuerst sicher, dass Sie *Instant Message Blocking* **aktiviert** haben. Danach wählen Sie die Checkboxe/n Yahoo und/oder MSN Messenger aus.
Peer to Peer Blocking	Voreingestellt ist **Deaktiviert**. **Deaktiviert:** Die P2P Sperrung ist deaktiviert. **Ständig verbunden:** Die P2P Sperrung ist aktiviert. **TimeSlot1 ~ TimeSlot16:** Dies ist der benutzerdefinierte Zeitschlitz. Für eine detaillierte Beschreibung wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
BitTorrent / eDonkey	Stellen Sie zuerst sicher, dass Sie *Peer to Peer Blocking* **aktiviert** haben. Danach wählen Sie die Checkboxe/n BitTorrent und/oder eDonkey aus.

5.3.6.6 Firewall Log

Das Firewall Log zeigt Log Informationen von unerwarteten Ereignissen, die von Ihrer Firewall festgestellt wurden.



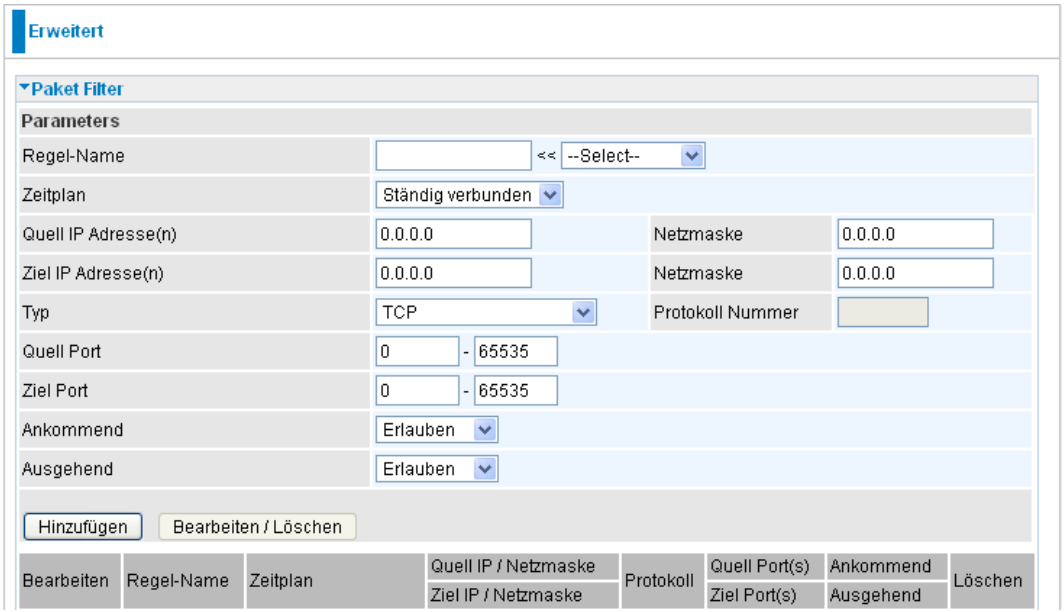
Wählen Sie einen oder mehrere **Aktivieren** Radio Button(s), um die Log(s) zu aktivieren. Die Log Information wird im System Log protokolliert; das wird auf das Kapitel **5.6.9 System Log** verwiesen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.7. Jugendschutz

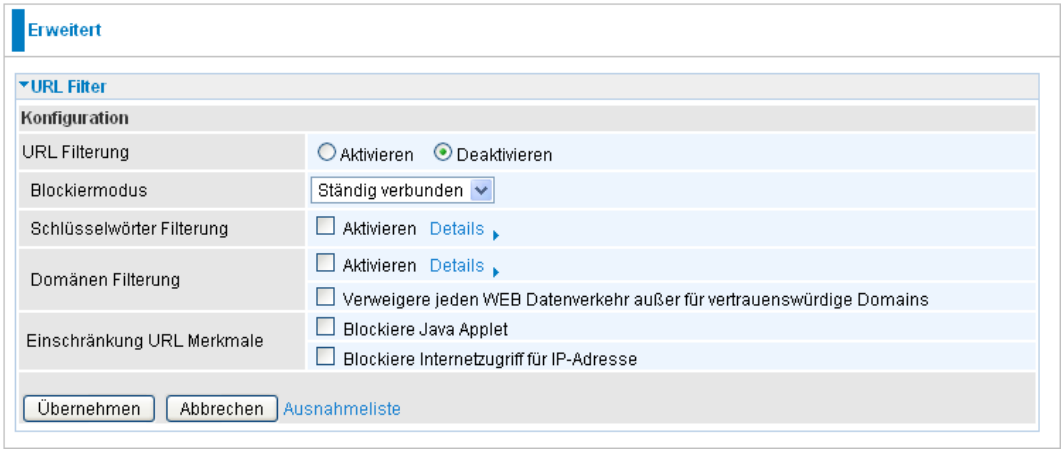
5.3.7.1 Zeitsperre

Für eine detaillierte Erklärung wird auf Kapitel **5.3.6.2 IP Filter** verweisen.



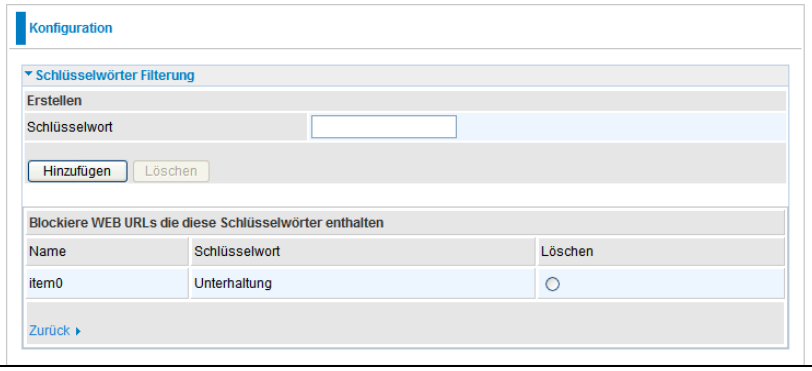
5.3.7.2 URL Filter

URL (Uniform Resource Locator, z.B. eine Adresse in der Form http://www.example.com) Filterregeln ermöglichen, Benutzern in Ihrem Netzwerk den Zugriff auf bestimmte Webseiten zu verbieten. Es sind keine URL Filterregeln voreingestellt. Sie können Filterregeln hinzufügen, um Ihre Anforderungen abzudecken.

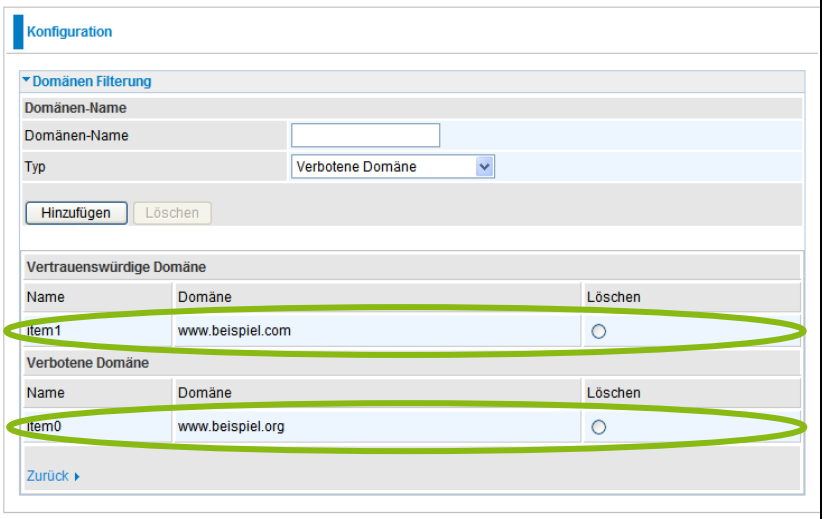


URL Filter	**Aktivieren/Deaktivieren:** Aktivieren oder deaktivieren Sie die URL Filter Funktion. Dadurch wird den Clients in Ihrem LAN Zugriff auf ungewollte Webseiten verhindert.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Blockiermodus	Voreingestellt ist **Ständig verbunden**. Listet vordefinierte Modi auf, um den URL Filter auszuwählen. **Deaktiviert:** Keine Aktion wird vom Blockiermodus ausgeführt. **Ständig verbunden:** Der URL Filter ist aktiviert. Die URL Filterregen werden ständig überwacht und überprüft. **TimeSlot1 ~ TimeSlot16**: Dies ist der benutzerdefinierte Zeitschlitz. Für eine detaillierte Beschreibung dazu, wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
Schlüsselwörter Filterung	Ermöglicht die Sperrung von Teilen von Webseiten für beliebige URLs ohne komplette URLs angeben zu müssen (z.B. um jegliche Bilder mit Werbung.gif zu sperren). Wenn die Funktion aktiviert ist, wird Ihre angegebene Schlüsselwörterliste mit der eingegebenen URL verglichen, um nachzusehen, ob Teile der angeforderten Seite blockiert werden soll. **Bemerkung:** Der URL Filter blockiert nur Webseitenanfragen (HTTP) über Port 80. ***Zum Beispiel***, wenn die URL http://www.example.com/Werbung.gif lautet, wird diese geblockt, weil Sie das Schlüsselwort 'Werbung' enthält. 

© Internetagentur Schott GmbH, 2010. All rights reserved.

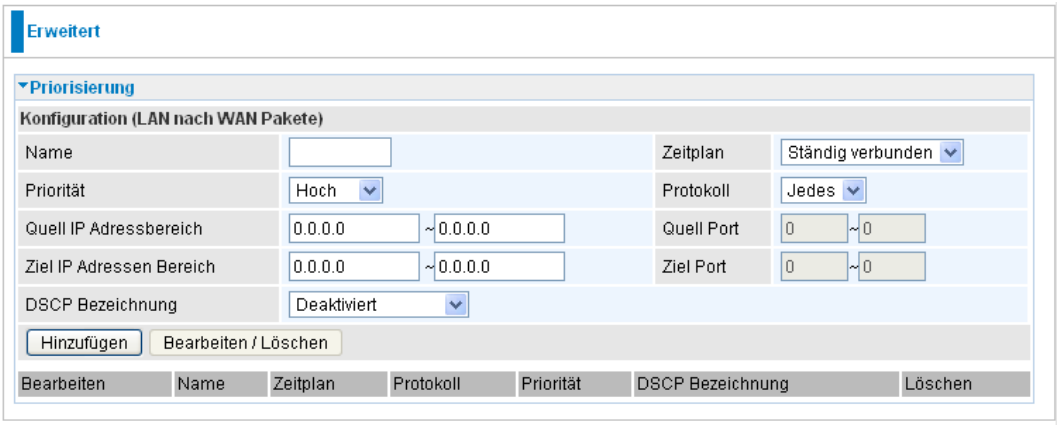
Domänen Filterung	Diese Funktion vergleicht die gesamte URL, nicht die IP Adresse, mit der URL Trusted Domain List (Vertrauenswürdige Domäne) und der Forbidden Domain List (Verbotene Domäne). Wenn eine Übereinstimmung vorliegt, wird die URL Anfrage gesendet (Trusted) oder verworfen (Forbidden). **Bemerkung:** Um den Zugriff nur auf Trusted Domains zu erlauben, müssen Sie **beide** Checkboxen auswählen. Die Prüfprozedur beinhaltet folgende Schritte: 1. Überprüfung, ob der Domänenname in der Trusted List vorhanden ist. Wenn ja, wird der Verbindungsversuch gesendet. 2. Wenn nicht, wird überprüft, ob der Domänenname in der Forbidden List ist. Wenn ja, wird der Verbindungsversuch verworfen. 3. Wenn der Domänenname in keiner der Listen steht, dann wird der Verbindungsversuch gesendet. 4. Beachten Sie, dass die gesamte URL eingetragen werden muss. Im untenstehenden Beispiel, wird die URL Anfrage für www.beispiel.com gesendet, weil Sie in der Trusted List steht, während die URL Anfrage für www.beispiel.org nicht gesendet wird, da diese in der Forbidden List steht. 
Einschränkung URL Merkmale	**Blockiere Java Applet:** Diese Funktion blockiert Webinhalte, die Java Applets enthalten. **Blockiere Internetzugriff für IP-Adresse:** Surfen via IP Adressen wird nicht erlaubt, d.h. nur Domänennamen werden als Eingabe akzeptiert. ***Bemerkung***: Um diese Funktion zu aktivieren, muss die Domänenfilterung aktiviert sein.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.8. QoS

Die QoS Funktion kontrolliert den Netzwerkverkehr für jede Anwendung des LAN (Ethernet und/oder Wireless) zum WAN (Internet). Es erleichtert die verschiedenen Qualitäten und Geschwindigkeiten für jede Anwendung festzulegen, wenn die ADSL Übertragungsgrenze des Gerätes ausgeschöpft ist.

5.3.8.1 Priorisierung



Name	Beschreibt den benutzerdefinierten Namen für jede Regel/Anwendung.
Zeitplan	Zeitplan für Ihre Priorisierung.
Priorität	Beschreibt die Priorität, die jeder Regel/Anwendung gegeben wurde. Voreingestellt ist Hoch; Sie können diese Einstellungen auf Ihre Anwendungen wie folgt anpassen: Hoch (60%), Normal (30%) und Niedrig (10%) des maximalen verfügbaren ADSL Datendurchsatzes.
Protokoll	Beschreibt den Namen des unterstützten Protokolls.
Quell IP Adressbereich	Beschreibt den Quell IP Adressbereich, der überwacht wird.
Quell Port	Beschreibt den Quell Portbereich, der überwacht wird.
Ziel IP Adressbereich	Beschreibt den Ziel IP Adressbereich, der überwacht wird.
Ziel Port	Beschreibt den Ziel Portbereich, der überwacht wird.
DSCP Bezeichnung	Die Differentiated Services Code Point (DSCP) Funktion befindet sich in den ersten 6 Bits des ToS Bytes. DSCP Maskierung erlaubt, bestimmten Applikationen eine höhere Priorität zuzuweisen, was wiederum Einfluss hat auf das DSCP Handling des nächsten Routers. Beachten Sie dazu die nachfolgende Tabelle:

DSCP Mapping Table	
ADSL IAD	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)

© Internetagentur Schott GmbH, 2010. All rights reserved.

Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Tabelle 2 DSCP Mapping Table

5.3.8.2 Geschwindigkeitsreduktion

5.3.8.2.1. Ausgehend

Mit der Geschwindigkeitsreduktion können Sie die Geschwindigkeit des IP Verkehrs reduzieren.
„Ausgehend“ meint Daten, die ins Internet gehen.

Name	Beschreibt den benutzerdefinierten Name für jede Regel.
Zeitplan	Zeitplan Ihrer Regel. Für eine detaillierte Erklärung wird auf Kapitel **5.6.8 Zeitplan** verwiesen.
Protokoll	Beschreibt den Namen des unterstützten Protokolls.
Bandbreite	Beschränkt die Geschwindigkeit des ausgehenden Verkehrs. Der eingegebene Wert limitiert die Geschwindigkeit der Anwendung auf den Wert multipliziert mit 32kbps.
Quell IP Adressbereich	Beschreibt den Quell IP Adressbereich, der überwacht wird.
Quell Port	Beschreibt den Quell Portbereich, der überwacht wird.
Ziel IP Adressbereich	Beschreibt den Ziel IP Adressbereich, der überwacht wird.
Ziel Port	Beschreibt den Ziel Portbereich, der überwacht wird.

5.3.8.2.2. Ankommend

Für eine detaillierte Erklärung wird auf Kapitel **5.3.8.2.1 Ausgehend** verwiesen.
„Ankommend“ meint Daten, die aus dem Internet kommen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.8.2.3. Beispiel

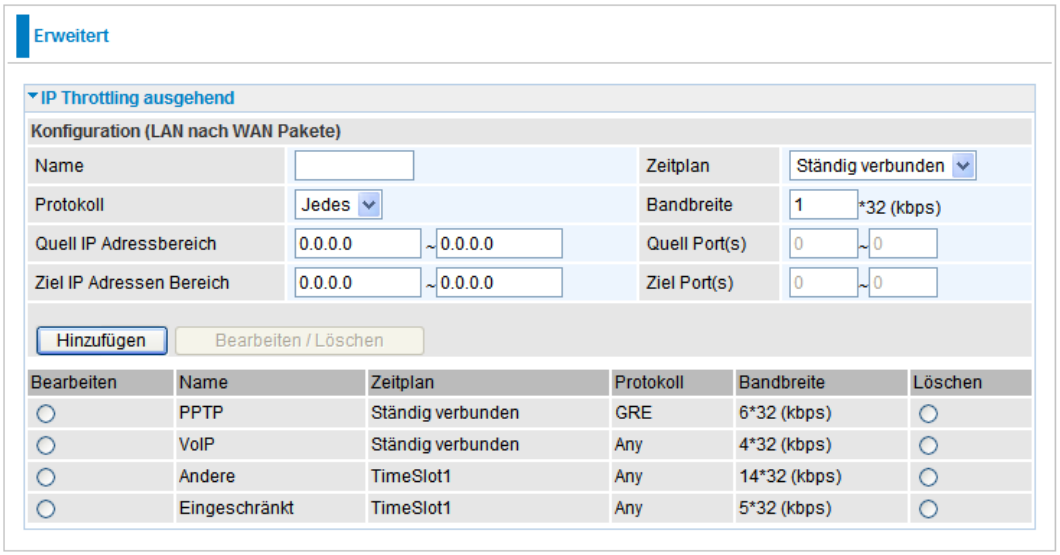
Mit der Geschwindigkeitsbegrenzung können Sie für die reservierte Bandbreite Details angeben.

Verfügbare Upstream Bandbreite: 928kbps (29*32kbps)

Die verfügbare Bandbreite soll wie folgt aufgeteilt werden:
Kritische Anwendung: 192kbps (6*32kbps)
Sprach Anwendung: 128kbps (4*32kbps)
Eingeschränkte Anwendung: 160kbps (5*32kbps)
Andere Anwendungen: 448kbps (14*32kbps)

Die Summe aller zugeteilten Bandbreiten darf die verfügbare Bandbreite nicht überschreiten.

6+4+14+5=29, 29*32kbps=928kbps

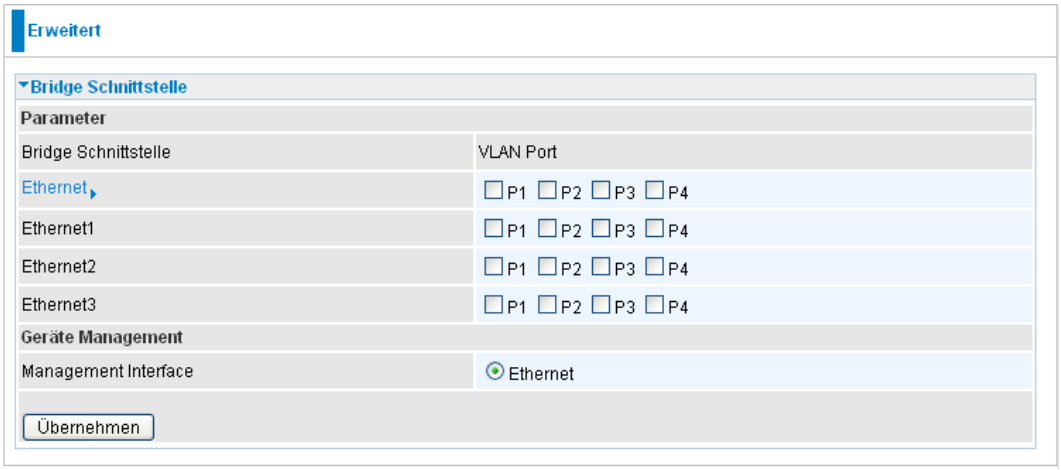


© Internetagentur Schott GmbH, 2010. All rights reserved.

5.3.9. Portzuordnung (Experten)

5.3.9.1 Portzuordnung

Auf dieser Seite können Sie Ihre Ethernet Ports aufsplitten, um virtuelle LANs (VLANs) zu erstellen. VLANs werden erstellt, um ein Netzwerk zu segmentieren. Dies ist hilfreich, wenn Anwendungen hohe Netzwerklast generieren (z.B. Video on Demand oder wenn eine Set-Top-Box am Gerät angehängt ist).

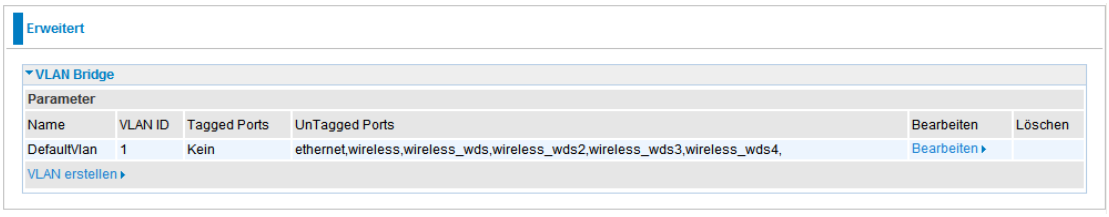


Management Interface: Gibt an, welche Gruppe von VLAN Port(s) das Gerät verwalten darf.

Bemerkung	**NAT/NAPT ist nur für das Management Interface verfügbar.** **Um die bridged Interfaces zu trennen, müssen Sie auch diese in den VLAN Bridge Einstellungen editieren. Dazu wird auf Kapitel 5.3.9.2 VLAN Bridge verwiesen.**

5.3.9.2 VLAN Bridge

Diese Seite ermöglicht Ihnen, VLAN Gruppe(n) zu erstellen und deren Mitglieder anzugeben.

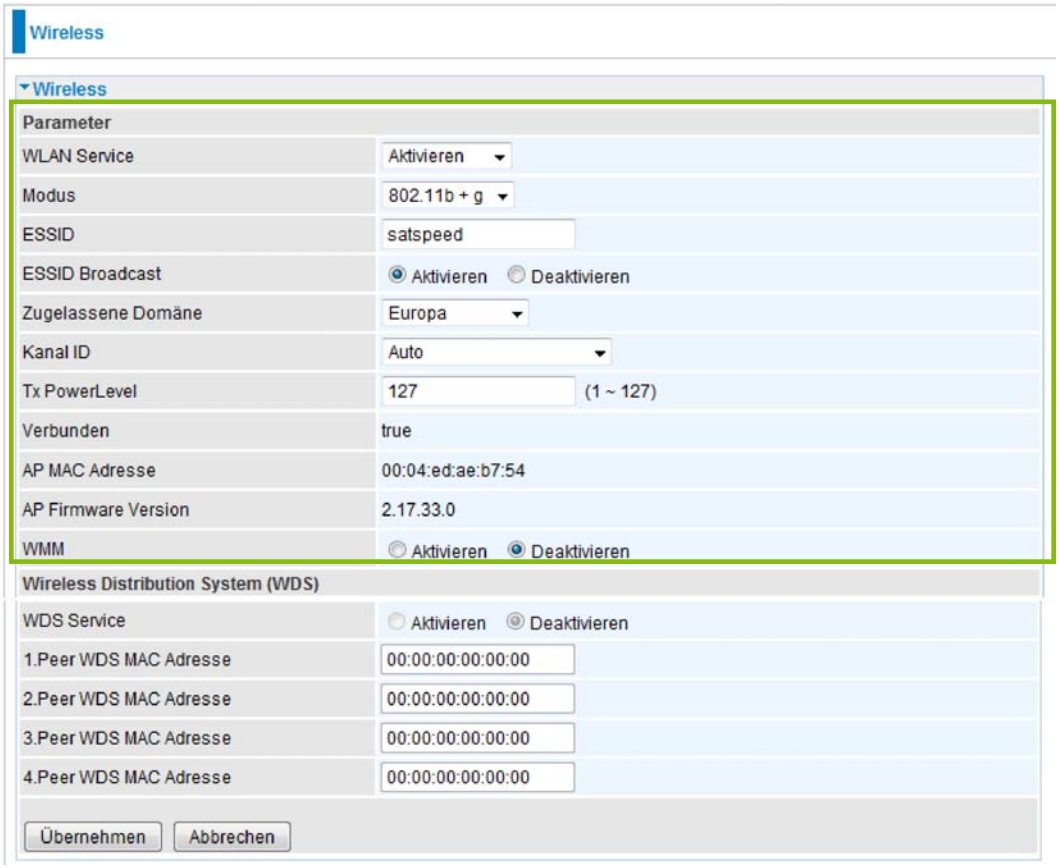


Bearbeiten	Bearbeiten Sie die zugehörigen Ports der ausgewählten VLAN Gruppe. Um Ethernet Ports zu trennen, müssen Sie diese zuerst einem anderem Netzwerk zuteilen. Dazu wird auf Kapitel **5.3.9.1 Portzuordnung** verwiesen. Entfernen Sie das entsprechende Netzwerk (ethernet+*index*) vom Standard VLAN (**DefaultVlan**) und erstellen Sie ein neues VLAN.
VLAN erstellen	Damit erstellen Sie eine neue VLAN Gruppe.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.4. Wireless

5.4.1. Grundeinstellungen



WLAN Service	Voreingestellt ist **Aktiviert**. Wenn Sie keine Wireless Clients im Netzwerk haben, wählen Sie **Deaktivieren**. Sie können auch einen „TimeSlot“ (Zeitschlitz) wählen, um das Wireless nur zur definierten Zeit zu aktivieren. Näheres dazu finden Sie im Kapitel **5.6.8 Zeitplan**.
Modus	Voreingestellt ist **802.11b+g** (Mixed mode). Wenn Sie nicht wissen, welcher Modus von Ihren Clients verwendet wird, dann bleiben Sie bei dieser Voreinstellung. Wählen Sie **802.11g**, wenn Sie nur 11g Clients im Netzwerk haben. Wählen Sie **802.11b**, wenn Sie nur 11b Clients haben.
ESSID	Die ESSID ist der eindeutige Name des Wireless Access Point (AP). Aus Sicherheitsgründen muss diese ESSID eindeutig sein. Stellen Sie sicher, dass Ihre Clients dieselbe ESSID wie das Gerät verwenden, damit sie sich mit Ihrem Wireless Netzwerk verbinden können. **Bemerkung:** Es wird zwischen Gross- und Kleinschreibung unterschieden und der Name darf nicht länger als 32 Zeichen sein.

© Internetagentur Schott GmbH, 2010. All rights reserved.

ESSID Broadcast	Voreingestellt ist **Aktiviert**. Zeigt oder versteckt Ihr Netzwerk. **Deaktiviert:** Die ESSID wird nicht ausgestrahlt. Ein Client, der die Netzwerke in der Umgebung absucht, findet das Netzwerk Ihres Gerätes nicht. **Aktiviert:** Ein Client, der die Netzwerke in der Umgebung absucht, findet das Netzwerk Ihres Gerätes.
Zugelassene Domäne	Sie können Ihr Land auswählen. Das ausgewählte Land bestimmt die zugelassenen Kanäle.
Kanal ID	Voreingestellt ist **Kanal 1**. Wählen Sie den Kanal, den Sie benutzen möchten. **Bemerkung:** Die Wireless Performance kann von einem anderen Wireless Netzwerk in der Umgebung beeinflusst werden, wenn auf dem selben Kanal gesendet wird.
TX PowerLevel	Voreingestellt ist **127** (Maximum). Diese Funktion ändert die Signalstärke. Benutzer können diesen Wert der Sendeleistung von 1 bis 127 anpassen.
Verbunden	Zeigt die Verbindung zwischen dem Gerät und der eingebauten Wireless Karte an, dargestellt in **true** (Verbunden) oder **false** (nicht verbunden).
AP MAC Address	Die Hardware Adresse des Access Points
AP Firmware Version	Die Firmware Version des Access Points
WMM	Voreingestellt ist **Deaktiviert**. WMM (Wi-Fi Multimedia) ist eine Wireless Quality of Service Einstellung. Diese ist hilfreich, wenn Sie Multimedia Services wie VoIP oder Video over IP benutzen.

5.4.2. Sicherheit

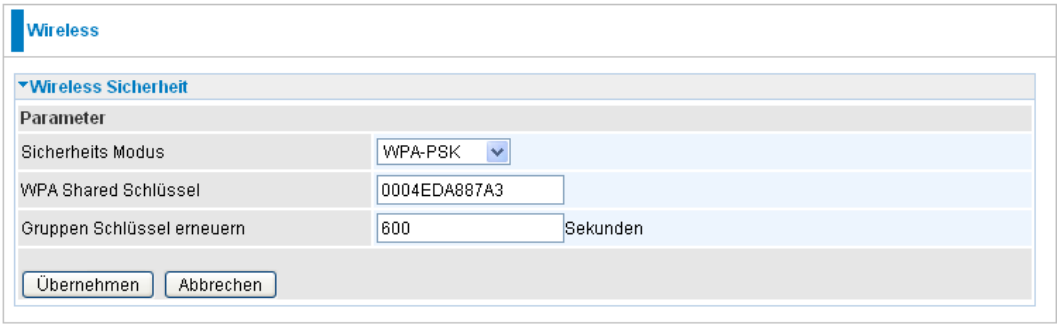
Wenn Sie das Wireless Netzwerk benutzen, empfehlen wir Ihnen, die Sicherheit einzuschalten, um das Netzwerk vor unerlaubtem Zugriff zu schützen. Klicken Sie dazu entweder auf „Standard Sicherheit“ oder „WPS“, um Ihr Netzwerk vor Eindringlingen zu schützen.
Mittels der Seite „Standard Sicherheit“ können Sie die Wireless Sicherheit manuell konfigurieren. WPS hingegen, ermöglicht es Ihnen, die Sicherheitseinstellungen automatisch vorzunehmen.

5.4.2.1 Standard Sicherheit

Die Seite „Standard Sicherheit“ erlaubt Ihnen Ihre Wireless Sicherheit manuell einzurichten. Sie können zwischen WPA-PSK, WPA2-PSK oder WEP wählen, um Ihr Wireless Netzwerk zu schützen oder die Sicherheit auszuschalten (was nicht empfohlen wird).
Voreingestellter Modus für die Wireless Sicherheit ist **WPA-PSK**.

© Internetagentur Schott GmbH, 2010. All rights reserved.

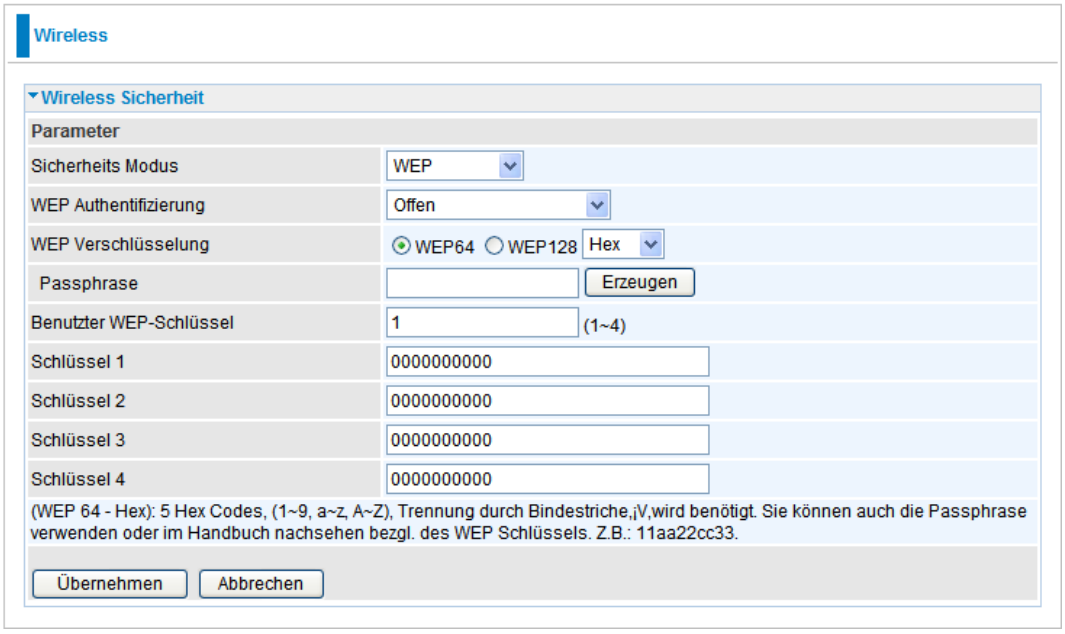
5.4.2.1.1. WPA-PSK / WPA2-PSK



Sicherheits Modus	Es gibt 2 WPA Sicherheitstypen: WPA-PSK und WPA2-PSK. WPA2-PSK ist sicherer als WPA-PSK. Jedoch kann es sein, dass WPA2-PSK nicht von jedem Wireless Client unterstützt wird.
WPA Shared Schlüssel	Voreingestellt ist ein eindeutiger Schlüssel, den Sie auf der Unterseite Ihres Gerätes vorfinden. Dieser ist der Schlüssel zur Netzwerkauthentifizierung. Sie können diesen Wert ändern. Die Eingabe erlaubt Zeichen (Gross-/ Kleinschreibung beachten, a-z, A-Z, 0-9) und die Länge sollte zwischen 8 und 63 Zeichen liegen.
Gruppen Schlüssel erneuern	Voreingestellt sind **600** Sekunden. Hier definieren Sie die Zeitspanne, nach der der Schlüssel automatisch zwischen den Wireless Clients und dem Access Point (AP) geändert wird.

5.4.2.1.2. WEP

Der WEP Verschlüsselungsmodus ist heutzutage nicht mehr sicher und kann einfach gehackt werden. Er wird nur noch unterstützt, um die Kompatibilität mit älteren Clients ohne WPA Verschlüsselung sicherzustellen.



© Internetagentur Schott GmbH, 2010. All rights reserved.

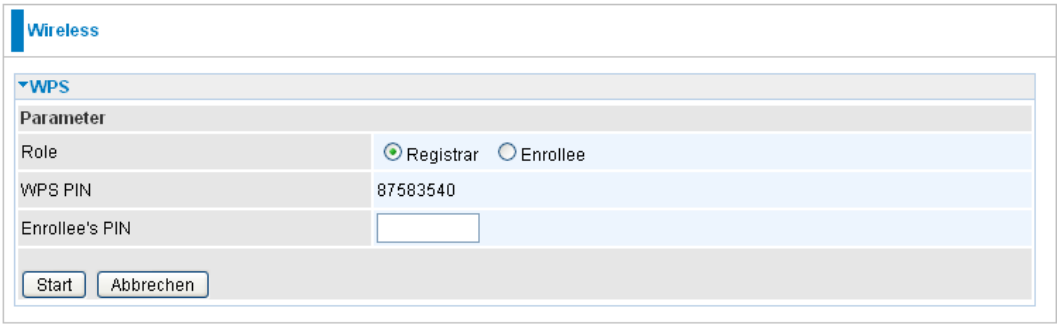
WEP Authentifizierung	Dieses Feld beinhaltet zwei Optionen: **Offen** und **Gemeinsam verwendet**. Wenn möglich, benutzen Sie **Offen,** da es sicherer als **Gemeinsam verwendet** ist.
WEP Verschlüsselung	WEP64 und WEP128 zeigen die Schlüssellänge. WEP128 benutzt einen 13 ASCII-Zeichen langen Schlüssel (26 in Hex). Infolgedessen ist es schwieriger, in ein solch verschlüsseltes Netzwerk einzudringen, als in ein WEP64 verschlüsseltes, welches eine ASCII-Zeichenlänge von 5 Zeichen (10 in Hex) benutzt.
Passphrase	Diese Funktion generiert aufgrund eines eingegebenen Texts und einem vordefinierten Algorithmus einen WEP64 oder WEP128 Schlüssel. Geben Sie dazu einen Text ein und drücken Sie auf **Erzeugen**.
Benutzter WEP Key	Wählen Sie den Schlüssel aus den folgenden **Schlüssel (1-4)** aus.
Schlüssel (1-4)	Geben Sie den Schlüssel zur Wireless Verschlüsselung ein. Um verschlüsselte Datentransfers zu erlauben, müssen sowohl der Schlüssel auf dem Gerät, als auch die Schlüssel der Clients exakt übereinstimmen. Sie können bis zu 4 Schlüssel definieren.

© Internetagentur Schott GmbH, 2010. All rights reserved.

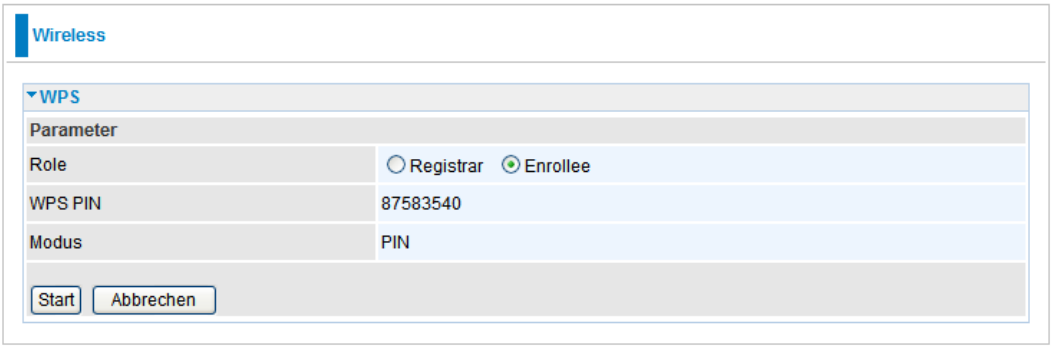
5.4.2.2 WPS

WPS ermöglicht eine einfache Einrichtung der Wireless Sicherheit.

5.4.2.2.1. PIN



Role	Ein Registrar (beispielsweise ein Access Point / Wireless Router, Computer oder anderes Gerät) entdeckt ein neues WPS Gerät in seiner Umgebung. Der Benutzer wird dann aufgefordert die PIN einzugeben, um das Gerät ins Netzwerk aufzunehmen. In diesem Modus verschlüsselt das WPS Netzwerk die Daten und authentifiziert jeden Client in seinem Netzwerk. Die „PIN Methode“ ist in allen WPS Clients vorhanden.
WPS PIN	Das ist die PIN Ihres Access Points, die ein Client bei sich eingeben muss, um sich mit dem Access Point zu verbinden.
Enrollee’s PIN	Dies ist die PIN Ihres Clients und diese muss beim Access Point eingegeben werden, um sich mit dem/n Client/s zu verbinden.



Role	In der Rolle des Enrolee meldet sich dieses Gerät bei einem anderen Access Point an. In der Enrolee-Role müssen Sie die WPS PIN, die untern angezeigt wird, beim verbindenden Client eingeben und danach klicken Sie auf beiden Seiten (Enrolee und Registrar) den **Start** Button, um die Autorisierung und Verschlüsselung der Daten zu starten. Dieser Modus ist in allen WPS Clients verfügbar.
WPS PIN	Dies ist die PIN Ihres Access Points und Ihr Client benötigt diese, um mit dem Access Point zu verbinden.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.4.2.2.2. WPS Knopf

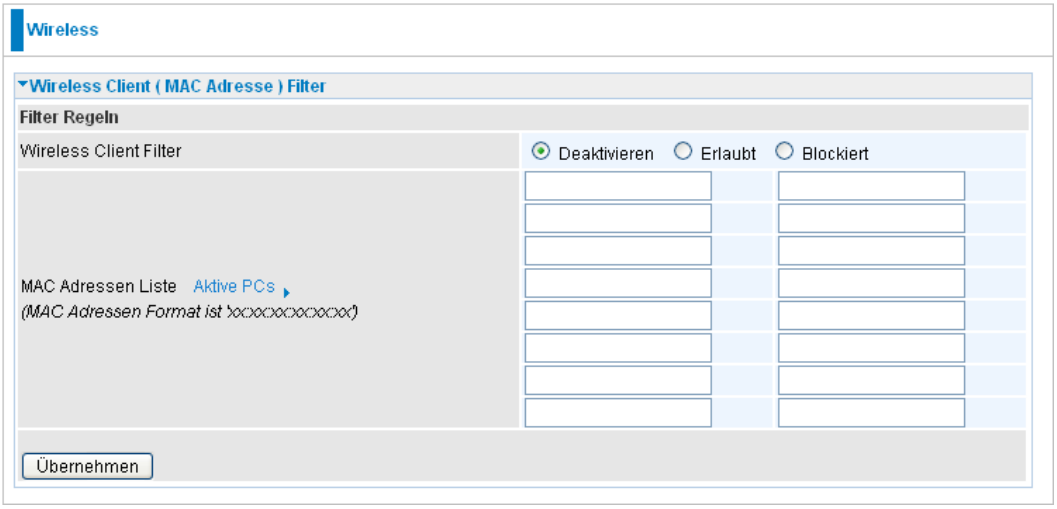
Sie können mehrere Clients mit dem Access Point (AP) verbinden, indem Sie die WPS Knöpfe drücken – sowohl beim AP als auch bei den Clients – um die Datenverschlüsselung einzuschalten. Das Gerät hat einen WPS Knopf auf der Rückseite (siehe Abbildung). Die Clients können ebenfalls einen Knopf haben oder über eine Software verfügen, die diese Funktion ermöglicht.
Es besteht die Möglichkeit, dass während der Einrichtungszeit von zwei Minuten, nicht berechtigte Clients sich ebenfalls mit dem Netzwerk verbinden können, sofern diese gleichzeitig einen Verbindungsversuch unternehmen.

Drücken Sie den Knopf kürzer als 5 Sekunden, um WLAN Clients mit WPS hinzuzufügen.
Drücken Sie den Knopf länger als 5 Sekunden, um das WLAN zu aktivieren/ deaktivieren.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.4.3. Zugangskontrolle

Die Zugangskontrolle (MAC Filter) unterstützt bis zu 16 Wireless Netzwerk Clients und erlaubt entweder Datenverkehr von autorisierten Clients anzunehmen oder von ungewünschten Clients abzublocken.
Es sind keine voreingestellten MAC Adressen-Filterregel.

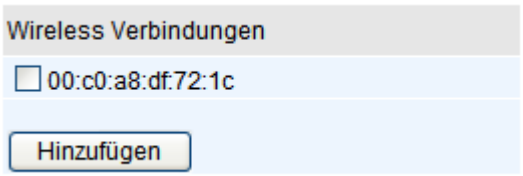


Wireless Client Filter	Voreingestellt ist **Deaktiviert**.
	Erlaubt: Klicken Sie diesen Radio Button, um Clients den Zugriff auf Ihr lokales Netzwerk zu erlauben, indem Sie deren MAC Adressen in die Zeilen eintragen. Oder klicken Sie Aktive PCs, um eine Liste der aktuell verbundnen Clients anzuzeigen. Stellen Sie sicher, dass MAC Adressen Ihrer PCs aufgelistet sind.
	Blockiert: Klicken Sie diesen Radio Button, um unerwünschten Zugriff von Clients auf Ihr lokales Netzwerk zu verbieten, indem Sie deren MAC Adressen in die Zeilen eintragen. Oder klicken Sie Aktive PCs, um eine Liste der aktuell verbundnen Clients anzuzeigen. Stellen Sie sicher, dass MAC Adressen Ihrer PCs **nicht** aufgelistet sind.
Aktive PCs Aktive PCs	Hier werden die Clients, die mit Ihrem Gerät per WLAN verbunden sind, aufgelistet. Nähere Informationen dazu finden Sie im Kapitel **5.4.3.1 Aktive PCs – Wireless Verbindungen**

Die maximale Anzahl Clients beträgt 16. Die MAC Adressen sind 6 Bytes lang; sie bestehen nur aus hexadezimalen Zeichen. Die Ziffern 0-9 und a-f werden somit akzeptiert.
Bemerkung: Befolgen Sie das übliche Format von MAC-Adressen xx:xx:xx:xx:xx:xx. Der Doppelpunkt (:) ist Teil dieses Formates.

© Internetagentur Schott GmbH, 2010. All rights reserved.

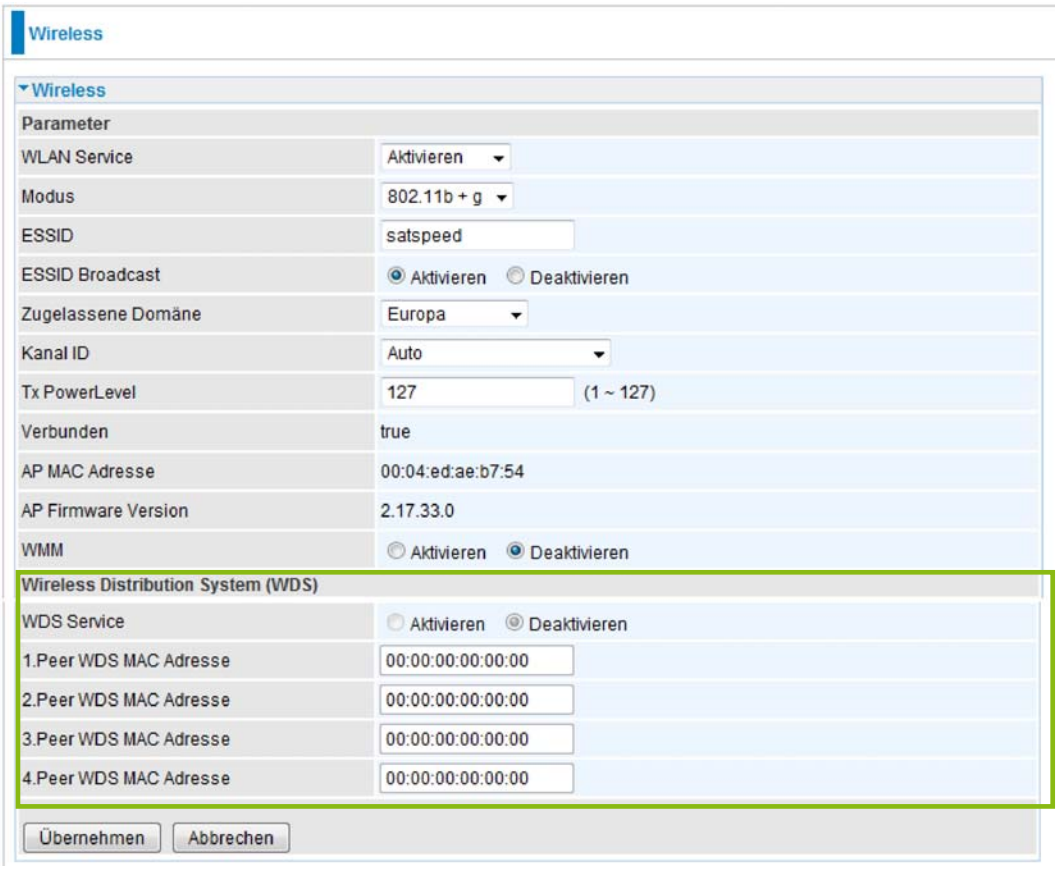
5.4.3.1 Aktive PCs – Wireless Verbindungen



Wireless Verbindungen ist eine Liste der MAC Adressen der mit dem Access Point verbundenen Netzwerkclients.
Klicken Sie die Checkbox eines aufgelisteten Clients an, und danach auf **Hinzufügen**, um den Client in die MAC Adressliste aufzunehmen.

5.4.4. Signalverstärker (Repeater)

Diese Funktion erweitert den Empfangsbereich des Wireless Netzwerkes. Es können bis zu 4 Wireless APs miteinander verbunden werden, um den Empfangsbereich zu vergrössern. Geben Sie die MAC Adressen der zusätzlich zu verbindenden Wireless Repeater ein.



WDS Service	Voreingestellt ist **Deaktiviert**. Klicken Sie auf den **Aktivieren** Radio Button, um die Funktion einzuschalten.

© Internetagentur Schott GmbH, 2010. All rights reserved.

#. Peer WDS MAC Adresse	Dies ist die MAC Adresse des verbundenen AP. Es ist wichtig, dass Ihr entfernter AP Ihre MAC Adresse enthält, um die Verbindung zu erlauben.

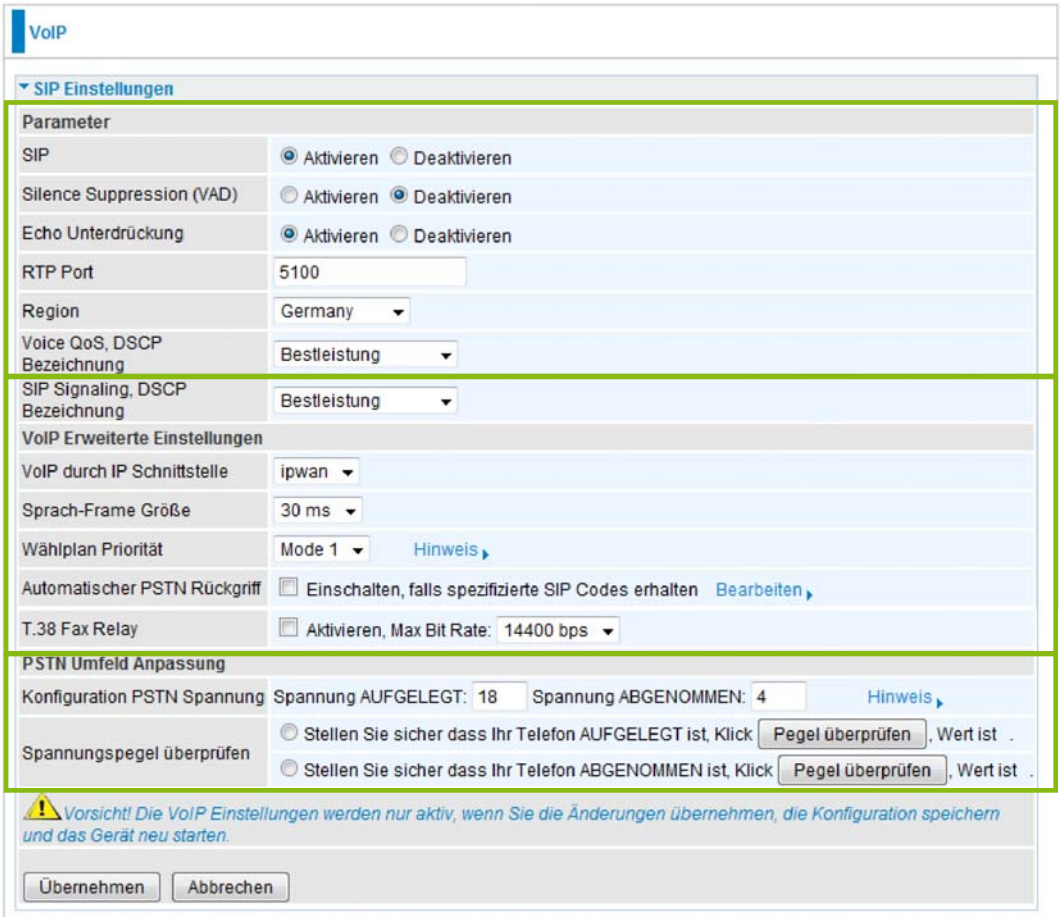
Bemerkung: Bei MAC Adressen muss der Doppelpunkt (:) enthalten sein.
WDS unterstützt nur WEP Verschlüsselung.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.5. VOIP

5.5.1. SIP Einstellungen (Experten)

Dieser Teil bietet eine einfache Einrichtung des VoIP Dienstes. Telefonanschluss 1 und 2 können auf verschiedene SIP Service Providers registriert werden.



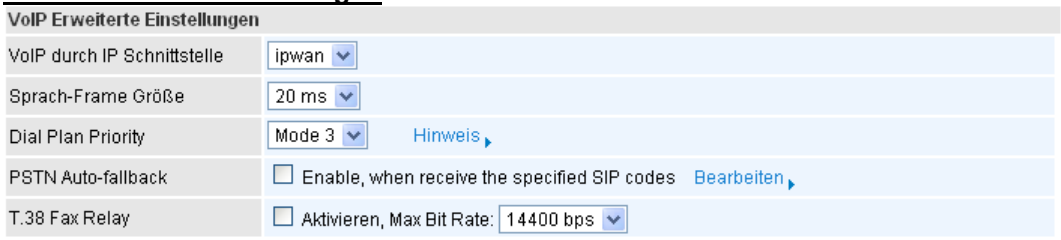
Vorsicht	Die folgend aufgelisteten Änderungen werden erst aktiv, wenn Sie die Änderungen übernehmen, die Konfiguration abspeichern und das Gerät neu starten: • **Deaktivieren von VoIP** (SIP) • Ändern des **VoIP durch IP Schnittstelle** • Ändern des **RTP Port**

© Internetagentur Schott GmbH, 2010. All rights reserved.

SIP Geräte Parameter

SIP	Voreingestellt ist **Deaktivieren**. Um die Internettelefonie zu benutzen (via SIP Protokoll), wählen Sie **Aktivieren**.
Silence Suppression (VAD)	Voreingestellt ist **Aktivieren**. Voice Activity Detection (VAD) ermöglicht eine effiziente Ausnutzung der Bandbreite. Es ist auch bekannt als Silence Suppression, die die Bandbreite nur dann reserviert, wenn gesprochen wird.
Echo Unterdrückung	Voreingestellt ist **Aktivieren**. G.168 Echo Unterdrückung ist ein ITU-T Standard. Diese Funktion verhindert Echo, während Sie sprechen.
RTP Port	Bereich von 5100 bis 65535, voreingestellt ist der Wert 5100. Geben Sie den Wert der Media Ports (RTP) an, die den verschiedenen Endpunkten zugewiesen werden und den verschieden Gesprächen, die möglicherweise existieren.
Region	In dieser Pull-Down Liste können Sie das Land wählen, in dem das VoIP Gerät benutzt wird. Dabei werden automatisch die länderspezifischen Parameter geladen.
Voice QoS, DSCP Bezeichnung	Differentiated Services Code Point (DSCP) befindet sich in den ersten 6 Bits des ToS Bytes. DSCP Maskierung erlaubt es, bestimmten Applikationen eine höhere Priorität zuzuweisen. **Bemerkung:** Stellen Sie sicher, dass die Router im Netzwerk diese Möglichkeit der Maskierung mittels DSCP unterstützen, um den Datenverkehr im QoS Netzwerk korrekt weiterzuleiten.

VoIP Erweiterte Einstellungen



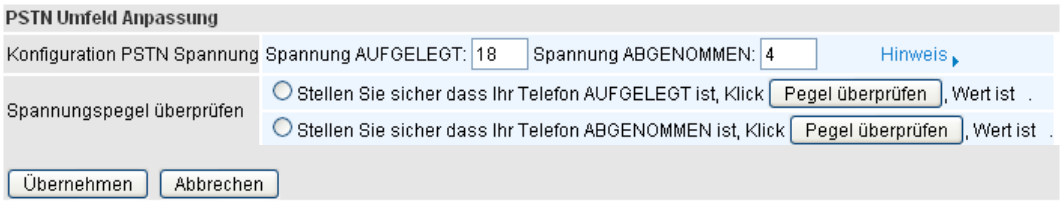
VoIP durch IP Schnittstelle	Die IP Schnittstelle spezifiziert, wo der VoIP Verkehr gesendet/empfangen wird: WAN (SIP Server bei dem ISP) oder LAN (Sie haben Ihren eigenen SIP Server)
Sprach-Frame Grösse	Die Frame Grösse reicht von 10 ms bis 60 ms. **Bei Internet via Satellit [satspeed/ Tooway usw.] 30ms**
Dial Plan Priority	Definiert die Priorität zwischen dem VoIP und dem PSTN Wählplan. Klicken Sie auf **Hinweis**, um sich die Möglichkeiten aufzeigen zu lassen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

PSTN Auto-fallback	Wenn VoIP nicht verfügbar ist, wechselt das Gerät automatisch auf PSTN. Klicken Sie auf **Bearbeiten**, um SIP Codes für einen Fallback hinzuzufügen oder zu löschen. Die Codes müssen mit einem Komma **(,)** getrennt werden. Für mehr Informationen über SIP Antwort Codes, klicken Sie auf Hier oder direkt auf: http://voip-info.org/wiki/view/sip+response+codes.
T.38 Fax Relay	Diese Funktion erlaubt die Übertragung von Fax zwischen 2 Standard-3-Gruppe Clients in Echtzeit über das Internet. Dies funktioniert allerdings nur, wenn beide Clients diese Funktion unterstützen und eingeschaltet haben.

PSTN Umfeld Anpassung

Mit der PSTN Umfeld Anpassung Option können Sie die Spannungswerte für die möglichen Zustände (aufgelegt, abgenommen) einstellen. Sie sollten diese nur ändern, wenn die Standardeinträge inkorrekt sind und somit die PSTN Anrufe nicht richtig erkannt werden.



Konfiguration PSTN Spannung	Geben Sie die Werte in die Felder ein.
Spannungspegel überprüfen	Beispiel: ABGENOMMEN-Check: Um den PSTN Spannungspegel zu überprüfen, nehmen Sie den Hörer ab und wählen 00#. Wenn Sie den PSTN Wählton hören, warten Sie einige Sekunden und drücken Sie dann auf den Button **Pegel überprüfen**. Für den AUFGELEGT-Check, drücken Sie auf den entsprechenden **Pegel überprüfen** Knopf.

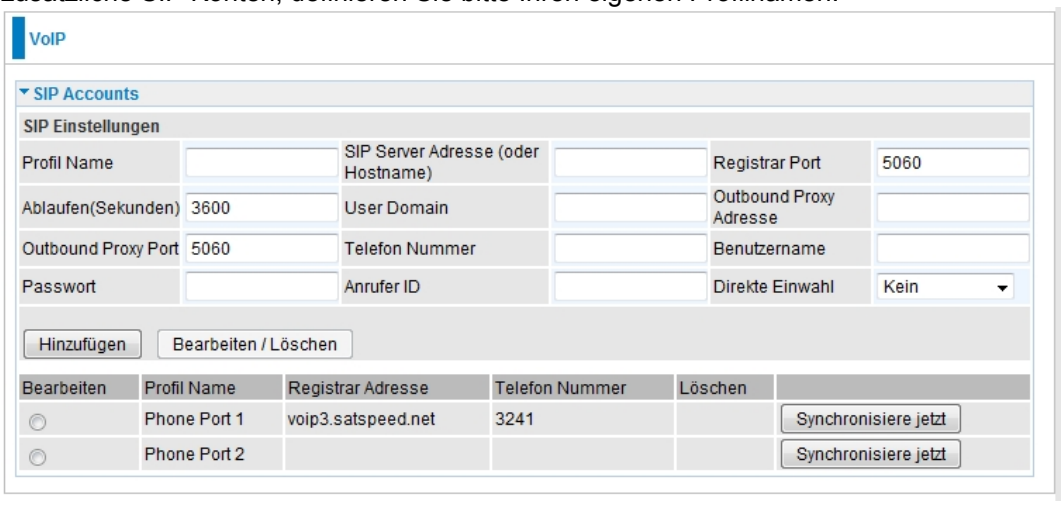
© Internetagentur Schott GmbH, 2010. All rights reserved.

5.5.2. SIP Konten

Auf dieser Seite können Sie Ihre SIP Konten konfigurieren und registrieren.
Sie können die SIP Konten auch im Schnellstart konfigurieren. Dazu wird auf Kapitel **5.2 Schnellstart** verwiesen.

Die ersten beiden SIP Konten müssen den Telefonanschlüssen 1 und 2 zugeordnet werden, um ausgehende Anrufe tätigen zu können. Wählen Sie dafür Telefonanschluss 1, geben die SIP Kontodaten ein und speichern Sie diese Änderungen mit dem **Bearbeiten/Löschen** Knopf. Dieselben Schritte gelten auch für den Telefonanschluss 2 und ihr zweites SIP Konto.
Sie können zusätzliche SIP Konten eingeben, indem Sie die dazu nötigen SIP Kontodaten eingeben und danach auf **Hinzufügen** klicken.

Hinweis: Die Profilname Phone Port 1 und Phone Port 2 stehen für die Telefonanschlüsse 1 und 2. Sie können weder verändert noch kopiert werden. Für zusätzliche SIP Konten, definieren Sie bitte Ihren eigenen Profilnamen.



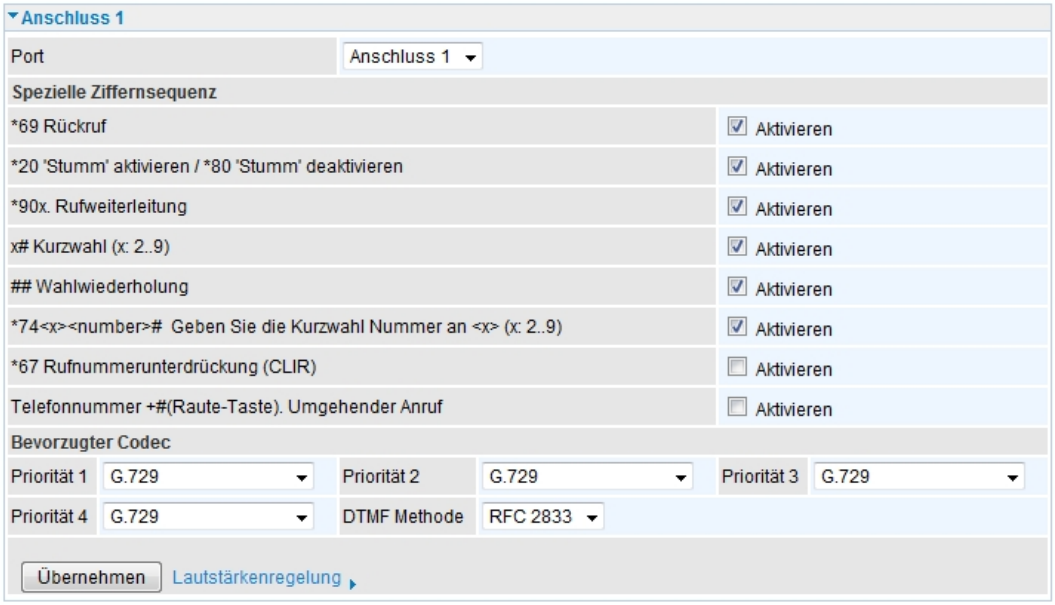
Profil Name	Vordefiniert für Telefonanschluss 1 und 2, für zusätzliche SIP Konten können Sie eigene Namen vergeben.
SIP Server Adresse (oder Hostname)	Beschreibt den SIP Registrar Server.
Registrar Port	Beschreibt den SIP Registrar Port. Ändern Sie diesen nur auf Anweisung Ihres SIP Providers.
Ablaufen(Sekunden)	Ablaufzeit der Registrierung.
User Domain	SIP Provider spezifischer Domänenname für den SIP Proxy Server.
Outbound Proxy Adresse	Beschreibt die Adresse des SIP Outbound Proxy Servers Ihres SIP Providers.
Outbound Proxy Port	Beschreibt den SIP Outbound Proxy Port.
Telefon Nummer	Beschreibt die Anmeldungsdaten Ihres SIP Kontos bei Ihrem SIP Provider. Geben Sie hier die von Ihrem SIP Provider erhaltenen Anmeldungsdaten ein.
Benutzername	
Passwort	
Anrufer ID	Dieser Wert wird beim Telefon des Angerufenen angezeigt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Direct in Dial	Wenn Sie mehr als zwei SIP Konten registrieren, geben Sie hier an, an welchem Telefonanschluss ankommende Anrufe läuten sollen.

5.5.3. Anschlusseinstellungen

Diese Seite zeigt die erweiterten Einstellungen des Telefonanschlusses an. Sie können Einstellungen für jeden einzelnen Anschluss definieren.



Port	Wählen Sie den zu bearbeitenden Telefonanschluss.
Spezielle Ziffernsequenz	Einige Tastencodes sind in dieser Tabelle schon voreingestellt. Wenn Sie Sie aktivieren, können Sie den Tastencode am ausgewählten Telefonanschluss verwenden, um die entsprechende Funktion auszuführen.
***69 Rückruf**	Wählen Sie *69, um die Nummer des letzten verpassten Anrufes zu wählen. Dies funktioniert nur für VoIP Anrufe.
***20 ‚Stumm' aktivieren**	Wählen Sie *20, um die Funktion „Stumm" („Bitte Nicht Stören") zu aktivieren. Ihr Telefon wird bei einem Anruf nicht klingeln.
***80 ‚Stumm' deaktivieren**	Wählen Sie *80, um diese Funktion wieder auszuschalten.
***90 <number> Rufweiterleitung**	Wählen Sie *90 gefolgt von einer Telefonnummer, um den Anruf zu einer anderen Nummer weiterzuleiten. Diese Funktion ist standardmässig eingeschaltet.
x# Kurzwahl	(x = 2…9) Der entsprechende Tastencode beschreibt eine Kurzwahlnummer, mit der die hinterlegte Rufnummer gewählt wird. Für eine detaillierte Erklärung wird auf Kapitel **5.5.7 Schnellwahl** verwiesen.
***74<x><number>#**	Benutzen Sie Ihre Telefontasten, um eine Telefonnummer als

© Internetagentur Schott GmbH, 2010. All rights reserved.

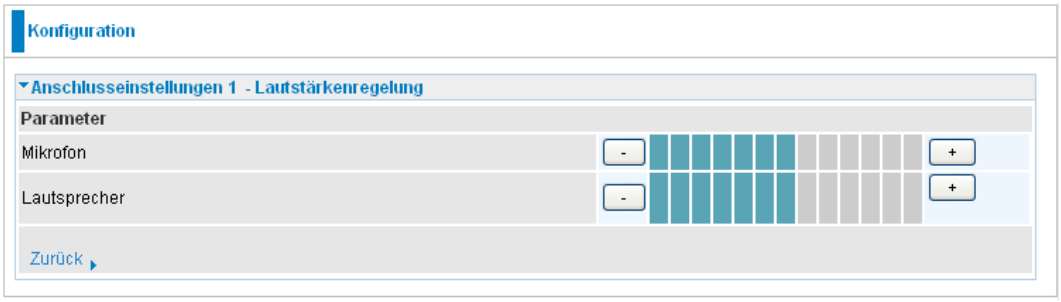
Geben Sie die Kurzwahlnummer an	Kurzwahl zu speichern. Sie können Ihre Kurzwahl Nummer manuell ändern. Für eine detaillierte Erklärung wird auf Kapitel **5.5.7 Schnellwahl** verwiesen.
## **Wahlwiederholung**	Drücken Sie ##, um Ihre letzte gewählte Nummer, nochmals anzurufen. Diese Funktion ist standardmässig eingeschaltet.
***67** **Rufnummerunter-drückung**	Unterdrücken Sie Ihre Rufnummer. Für den nächsten Anruf, den Sie tätigen, wird Ihre Nummer dem Angerufenen nicht angezeigt. Die detaillierte Sequenz ist: “Abnehmen -> *67 -> Auflegen -> Abnehmen -> Wählen”. Diese Funktion ist standardmässig ausgeschaltet.
<Telefonnummer> #	Um Wartezeiten nach dem Wahlvorgang zu vermeiden, drücken Sie nach Eingabe der Nummer #.

Bemerkung: Dieses Handbuch enthält eine komplette Liste aller Tastencodes. Dazu wird auf Kapitel **6.3 Anleitung für Zusatzdienste** verwiesen.
Bemerkung: x ist ein Platzhalter für eine Ziffer.

Bevorzugter Codec	Codec ist bekannt als Coder-Decoder, benutzt für die Datensignalumwandlung. Setzen Sie die Priorität für die Sprachkompression; Priorität 1 heisst höchste Priorität.
G.729	Diese Funktion codiert und decodiert Sprachinformationen in ein einzelnes Paket, welches den Bandbreitenverbrauch minimiert.
G.711µ-LAW	Diese Funktion ist eine nichtkomprimierende Encoder- und Decodertechnik. µ-LAW benutzt einen Pulse Code Modulation (PCM) Encoder/ Decoder, um lineare 14-Bit Samples zu konvertieren.
G.711A-LAW	Diese Funktion ist eine nichtkomprimierende Encoder- und Decodertechnik. µ-LAW benutzt einen Pulse Code Modulation (PCM) Encoder/ Decoder, um lineare 13-Bit Samples zu konvertieren.
G.726-32	Diese Funktion codiert und decodiert Sprachinformationen in ein einzelnes Paket, welches den Bandbreitenverbrauch minimiert. Momentan unterstützt diese Funktion nur Bitraten von 32Kbps.
DTMF Method	Inband, RFC 2833 und SIP INFO (RFC 2976) werden unterstützt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

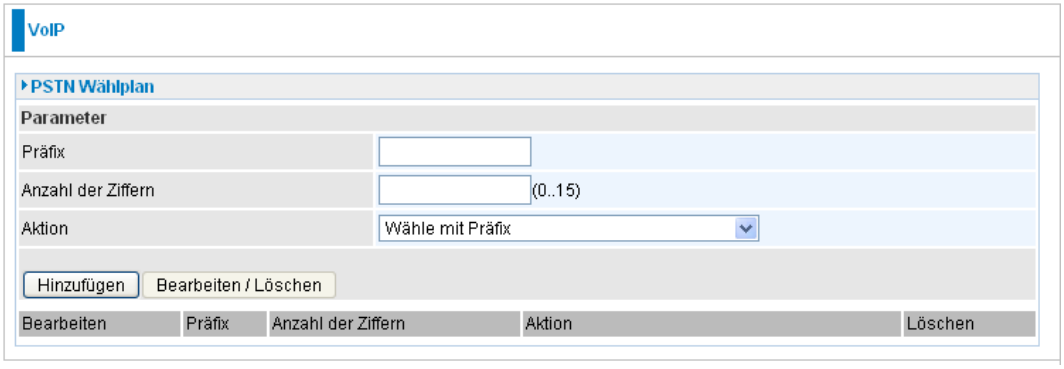
5.5.3.1 Lautstärkeregelung



Die Lautstärkeregelung hilft Ihnen, den Sprachlevel der Anschlüsse für eine optimale Wiedergabe anzupassen.
Drücken Sie auf „**-**“, das Minus-Symbol, um den Mikrofon- und/oder Lautsprecherlevel des Telefons zu senken.
Drücken Sie auf „**+**“, das Plus-Symbol, um den Mikrofon- und/oder Lautsprecherlevel des Telefons zu steigern.

5.5.4. PSTN Wählplan (Experten)

Sie können eine Liste mit Regeln erstellen, um Anrufe via PSTN anstelle VoIP zu tätigen. Die Auswahl basiert auf dem Präfix.
Bemerkung: Um diese Funktion zu nutzen, müssen Sie bei Ihrem SIP Server registriert und angemeldet sein und Sie müssen mit dem PSTN (Line Port) verbunden sein.



Präfix	Gibt die Ziffernfolge für die Benutzung des PSTN anstelle von VoIP an.
Anzahl der Ziffern	Gibt die Gesamtanzahl der Ziffern an, um raus zu wählen. Maximum Anzahl Ziffern ist 32.
Aktion	Gibt die Wählmethode an.
	Wähle mit Präfix: Die **mit** Präfix gewählte Nummer wird dem PSTN zugesandt.
	Wähle ohne Präfix: Die **ohne** Präfix gewählte Nummer wird dem PSTN zugesandt.
	Wählen nach Zeitüberschreitung: Die **mit** Präfix gewählte Nummer wird dem PSTN nach der Zeitüberschreitung zugesandt. Die Zeitüberschreitung tritt in Kraft, wenn eine bestimmte Zeit keine Ziffern mehr gewählt werden.

© Internetagentur Schott GmbH, 2010. All rights reserved.

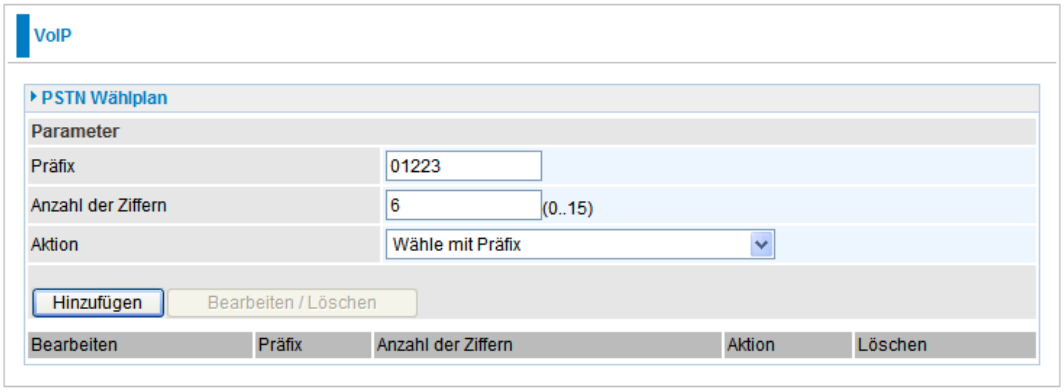
	Wählen nach Zeitüberschreitung ohne Präfix: Die **ohne** Präfix gewählte Nummer wird dem PSTN nach der Zeitüberschreitung zugesandt. Die Zeitüberschreitung tritt in Kraft, wenn eine bestimmte Zeit keine Ziffern mehr gewählt werden.

Bemerkung: Die gewählte Nummer darf die **Anzahl der Ziffern** nicht überschreiten.

Bemerkung	**Die Telefonanschlüsse 1 und 2 verweisen automatisch auf PSTN, wenn:** **- kein Strom vorhanden ist.** **- der Internet Service fehlschlägt, d.h. keine WAN IP Adresse mehr vorhanden ist.** **- die SIP Option deaktiviert ist. Dazu wird auf Kapitel 5.5.1 SIP Einstellungen (Experten) verwiesen.** **- Anrufe mit den Regeln im *PSTN Wählplan* übereinstimmen.** **- der SIP Service nicht erreichbar ist.**

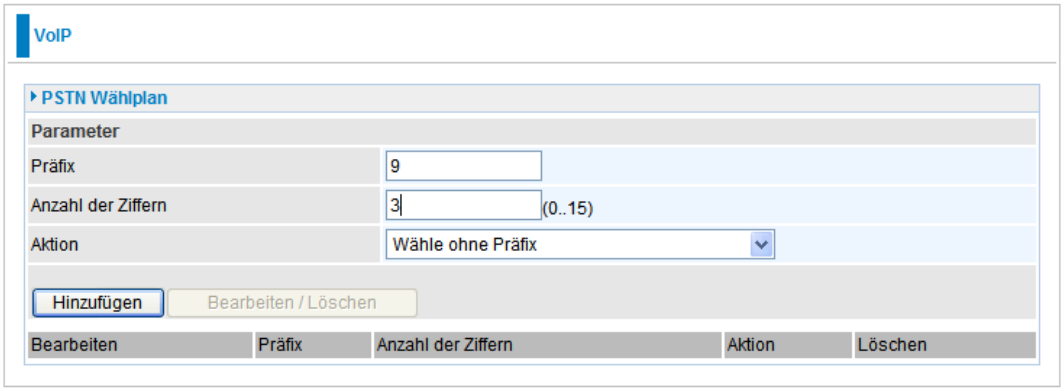
5.5.4.1 PSTN Wählplan Beispiele:

1) Wähle mit Präfix



Wenn Sie 01223 707070 wählen, wird die Nummer 01223707070 via Line Port gewählt, um einen regulären Anruf zu tätigen.

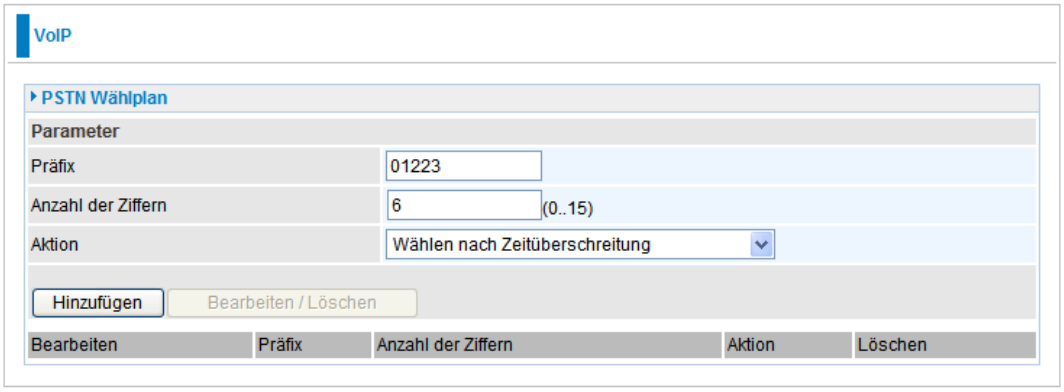
2) Wähle ohne Präfix



© Internetagentur Schott GmbH, 2010. All rights reserved.

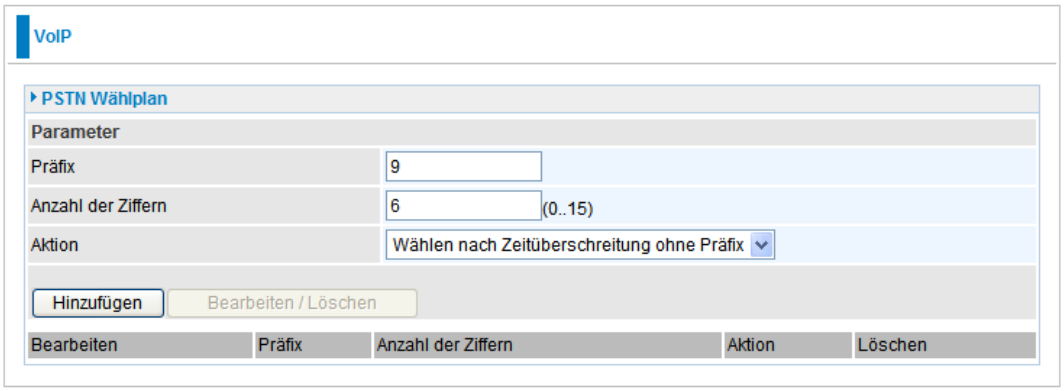
Wenn Sie 9102 wählen, wird nur die Nummer 102 via Line Port gewählt, um einen regulären Anruf zu tätigen.

3) Wählen nach Zeitüberschreitung



Wenn Sie nur 01223 7070 wählen und keine anderen Ziffern mehr, wird nach der Zeitüberschreitung 012237070 via Line Port gewählt, um einen regulären Anruf zu tätigen.
Obwohl 7070 (nur 4 Ziffern) nicht mit der Vorgabe im Feld übereinstimmen ist 7070 eine gültige Telefonnummer, solang Sie nicht 6 Ziffern überschreitet.

4) Wählen nach Zeitüberschreitung ohne Präfix

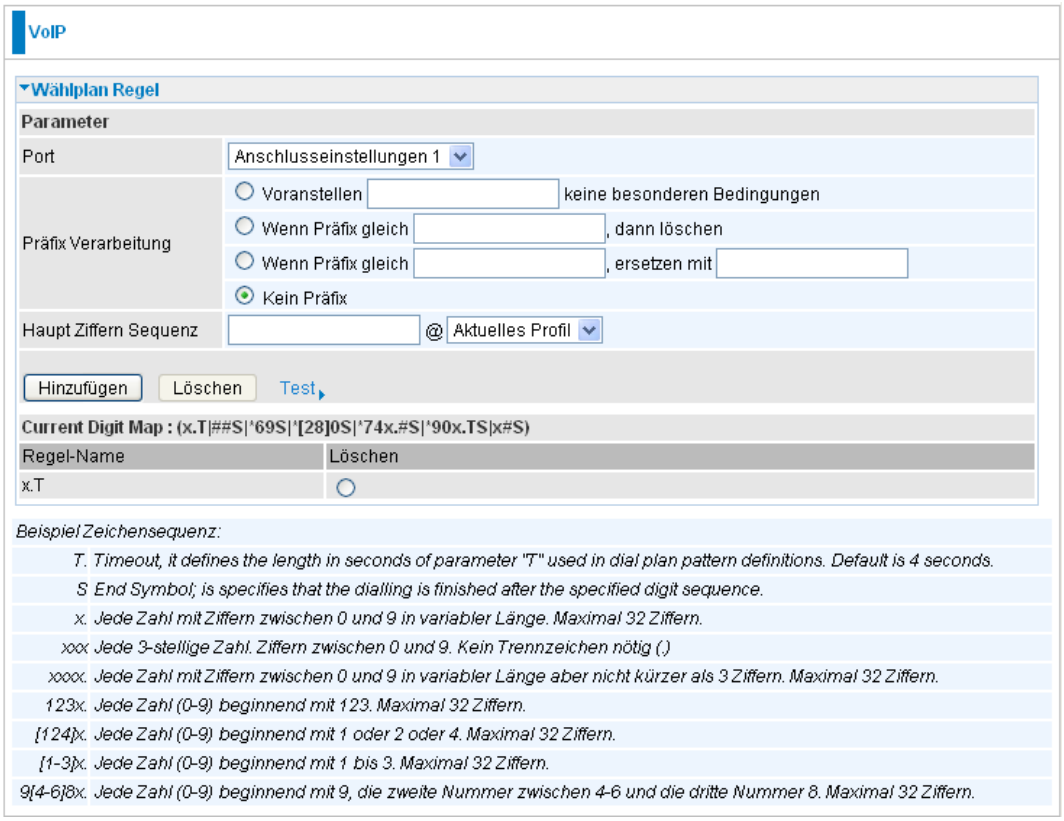


Wenn Sie 97070 wählen und keine anderen Ziffern mehr, wird nach der Zeitüberschreitung 7070 ohne Präfix via Line Port gewählt, um einen regulären Anruf zu tätigen.
Obwohl 7070 (nur 4 Ziffern) nicht mit der Vorgabe im Feld übereinstimmen ist 7070 eine gültige Telefonnummer, solang Sie nicht 6 Ziffern überschreitet.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.5.5. VOIP Wählplan (Experten)

Der VoIP Wählplan definiert Regeln für ausgehende Anrufe via VoIP pro Telefonanschluss.


VoIP
Wählplan Regel
Parameter
Port
Anschlusseinstellungen 1
Präfix Verarbeitung
Voranstellen
keine besonderen Bedingungen
Wenn Präfix gleich
, dann löschen
Wenn Präfix gleich
, ersetzen mit
Kein Präfix
Haupt Ziffern Sequenz
@
Aktuelles Profil
Hinzufügen
Löschen
Test
Current Digit Map : (x.T|##S|'69S|'[28]0S|'74x.#S|'90x.TS|x#S)
Regel-Name
Löschen
x.T
Beispiel Zeichensequenz:
T. Timeout, it defines the length in seconds of parameter "T" used in dial plan pattern definitions. Default is 4 seconds.
S End Symbol; is specifies that the dialling is finished after the specified digit sequence.
x. Jede Zahl mit Ziffern zwischen 0 und 9 in variabler Länge. Maximal 32 Ziffern.
xxx Jede 3-stellige Zahl. Ziffern zwischen 0 und 9. Kein Trennzeichen nötig (.)
xxxx. Jede Zahl mit Ziffern zwischen 0 und 9 in variabler Länge aber nicht kürzer als 3 Ziffern. Maximal 32 Ziffern.
123x. Jede Zahl (0-9) beginnend mit 123. Maximal 32 Ziffern.
[124]x. Jede Zahl (0-9) beginnend mit 1 oder 2 oder 4. Maximal 32 Ziffern.
[1-3]x. Jede Zahl (0-9) beginnend mit 1 bis 3. Maximal 32 Ziffern.
9[4-6]8x. Jede Zahl (0-9) beginnend mit 9, die zweite Nummer zwischen 4-6 und die dritte Nummer 8. Maximal 32 Ziffern.

Präfix Verarbeitung:

Voranstellen <Nummer> keine besonderen Bedingungen	<Nummer> ist der gewählten Nummer bedingungslos vorangestellt. Der Präfix kann irgendeine Nummer und/oder Buchstabe wie **+**, *****, **#** sein. **Bemerkung:** Für spezielle Services mit +, *, #, müssen Sie eventuell Ihren VoIP oder lokalen Telefon Service Provider kontaktieren.
Wenn Präfix gleich <Nummer>, dann löschen	Präfix <Nummer> wird bei einem Anruf von der gewählten Nummer entfernt.
Wenn Präfix gleich <Nummer1>, ersetzen mit <Nummer2>	Wenn Präfix <Nummer1> gewählt wird, wird er mit <Nummer2> ersetzt.
Kein Präfix	Kein Präfix wird vorangestellt.

Haupt Ziffern Sequenz:

x	Steht für beliebige Ziffern zwischen 0 und 9.
.	Steht für eine Wiederholung der vorhergehenden Ziffer.

© Internetagentur Schott GmbH, 2010. All rights reserved.

*	Steht für das normale '*' auf der Telefontastatur. Bitte überprüfen Sie, ob dies Ihr VoIP oder lokaler Telefon Service Provider unterstützt.
#	Steht für das normale '#' auf der Telefontastatur. Bitte überprüfen Sie, ob dies Ihr VoIP oder lokaler Telefon Service Provider unterstützt.
@ <>	
Aktuelles Profil	Bedeutet, dass Anrufe mit der eingegeben Sequenz das SIP Konto benutzen, das dem Telefonanschluss zugeordnet ist.(Phone Port 1 / Phone Port 2)
PSTN	Bedeutet, dass Anrufe mit der eingegeben Sequenz via PSTN abgewickelt werden (Line Port).
ENUM	Bedeutet, dass ein VoIP SIP Direktruf via E.164 Nummer ("ENUM") zu einem anderen ENUM Anschluss gemacht wird. Elektronische Nummer (ENUM) benutzt DNS (Domain Network System) Technologie, um eine herkömmliche Telefonnummer (PSTN) in eine Internetadresse/ SIP URL umzuwandeln. Die ENUM Nummer muss bei einer öffentlichen ENUM Seite oder Ihrem VoIP Service Provider registriert sein.
SIP-Konto	Dies ist ein Platzhalter für zusätzliche SIP Konten. Wenn Sie mehr als zwei SIP Konten definieren, werden Sie dessen Namen in der Liste sehen. Wenn Sie dieses SIP Konto wählen, wird es für Anrufe, die die Bedingungen auf der linken Seite erfüllen, verwendet. Um zusätzliche SIP Konten zu definieren, wird auf Kapitel **5.5.2 SIP Konten** verwiesen.

Klicken Sie auf **Hinzufügen**, um VoIP Wählplan Regel(n) hinzuzufügen.

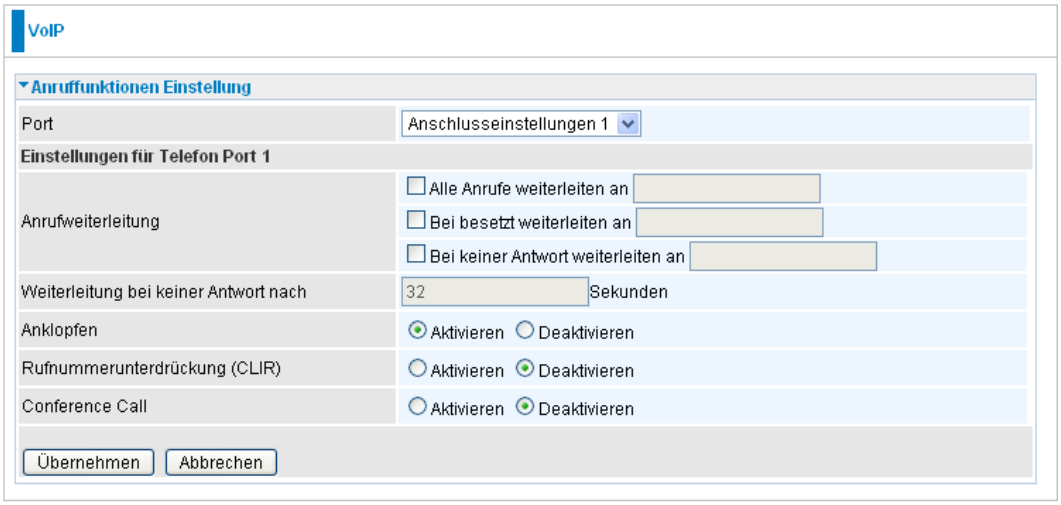
Zusätzliche Wählplan Beispiele:	**Beschreibung**
*xx*x.	Beginnt mit '* Zeichen' + 2 Ziffern + '* Zeichen' + eine Nummer (0-9) mit variabler Länge. Maximale Länge ist 32.
*xx	Beginnt mit '* Zeichen' + 2 Ziffern zwischen 0 und 9. Gesamtlänge inklusive * ist 3. Bemerkung: Es wird kein Wiederholungszeichen (.) verwendet.
**xx*x.	Beginnt mit '** Zeichen' + 2 Ziffern zwischen 0 und 9 + '* Zeichen' + eine Nummer (0-9) mit variabler Länger. Maximale Länge ist 32.
#xx.	Beginnt mit '# Zeichen' + eine Ziffernfolge (0-9) in variabler Länge aber nicht kürzer als 1 Ziffer. Maximale Länge ist 32.
##xx*x.	Beginnt mit '## Zeichen' + 2 Ziffern + '* Zeichen' + eine Nummer (0-9) mit variabler Länge. Maximale Länge ist 32.

Tabelle 3 Wählplan Beispiele

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.5.6. Anrufeinstellungen

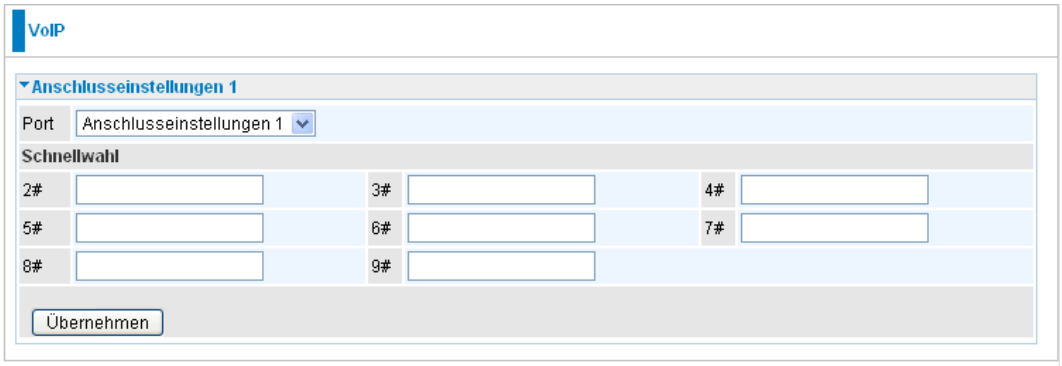
Anrufeinstellungen erlauben es Ihnen, das Verhalten des Gerätes bei ankommenden Anrufen oder während des Gespräches zu ändern. Das Gerät stellt Ihnen zum Beispiel eine Anrufweiterleitung zur Verfügung.
Diese Einstellungen müssen pro Telefonanschluss definiert werden. Um den betreffenden Telefonanschluss zu ändern, benutzen Sie das Pull-Down Menü.



Anrufweiterleitung	**Alle Anrufe weiterleiten an:** Diese Funktion erlaubt Ihnen alle Anrufe zur im nebenstehenden Feld angegebenen Nummer weiterzuleiten.
	Bei besetzt weiterleiten an: Diese Funktion erlaubt Ihnen eingehende Anrufe, während Sie bereits in einem anderen Gespräch sind, zur angegebenen Nummer weiterzuleiten.
	Bei keiner Antwort weiterleiten an: Diese Funktion erlaubt Ihnen eingehende Anrufe nach einer definierten Zeit (siehe nächste Zeile) zur angegebenen Nummer weiterzuleiten.
Weiterleitung bei keiner Antwort nach	Definieren Sie einen Zeitrahmen, in dem ein ankommender Anruf beantwortet werden muss, bevor er weitergeleitet wird. Dieses Feld steht im Zusammenhang mit dem vorherigen **Bei keiner Antwort weiterleiten an**.
Anklopfen	Aktivieren Sie hier die Anklopfen Funktion.
Rufnummerunterdrückung (CLIR)	Aktivieren Sie hier die Rufnummerunterdrückung. Dem angerufenen Teilnehmer, wird Ihre Nummer nicht übermittelt.
Conference Call	Aktivieren Sie hier die Konferenzschaltung.

© Internetagentur Schott GmbH, 2010. All rights reserved.

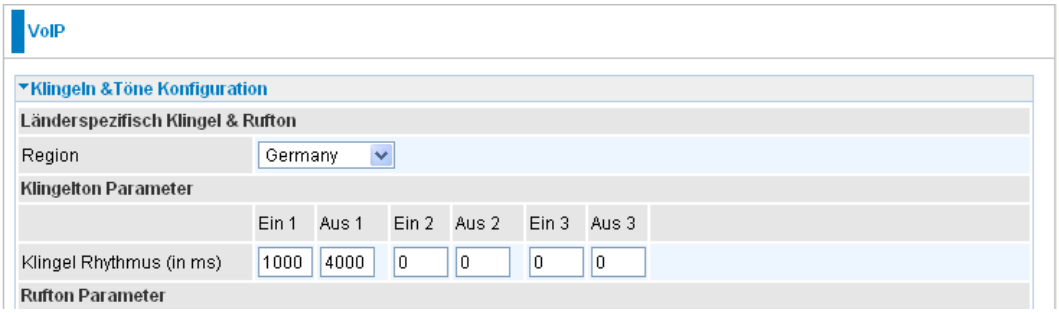
5.5.7. Schnellwahl



Schnellwahl erlaubt Ihnen beispielsweise die 2# zu wählen anstatt einer langen Telefonnummer. Die unter einer Schnellwahl gespeicherte Nummer steht im entsprechenden Feld.
Diese Schnellwahlnummern müssen für jeden Telefonanschluss einzeln angegeben werden.

5.5.8. Klingeln & Töne (Experten)

Diese Seite erlaubt Experten bestehende oder neue Parameter für die verschiedenen Klingeltöne (Wählton, Besetztton, usw.) zu ändern.



Länderspezifisch Klingel & Rufton
Region: Wählen Sie ein Land aus dem Pull-Down Menü. Danach werden länderspezifische Parameter automatisch geladen. Diese werden auch gleich nach der Auswahl automatisch angezeigt. Falls Ihr Land nicht in der Auswahl ist, können Sie die Parameter selbst editieren.

Klingelton Parameter
Klingel Rythmus (in ms): Klingel Rhythmus ist in 3 Felder unterteilt, Frequenz: Ein 1, Aus 1, Ein 2, Aus 2, Ein 3, Aus 3. Die Frequenz wird angegeben in Hertz und die Zeit ist in Millisekunden angegeben.

Rufton Parameter
Für diese Informationen müssen Sie Ihren lokalen Telefon Service Provider kontaktieren.

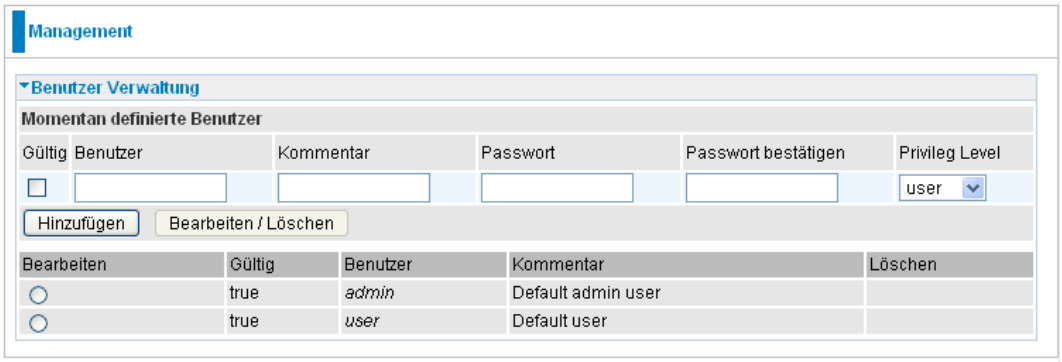
Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6. Management

5.6.1. Management Konten

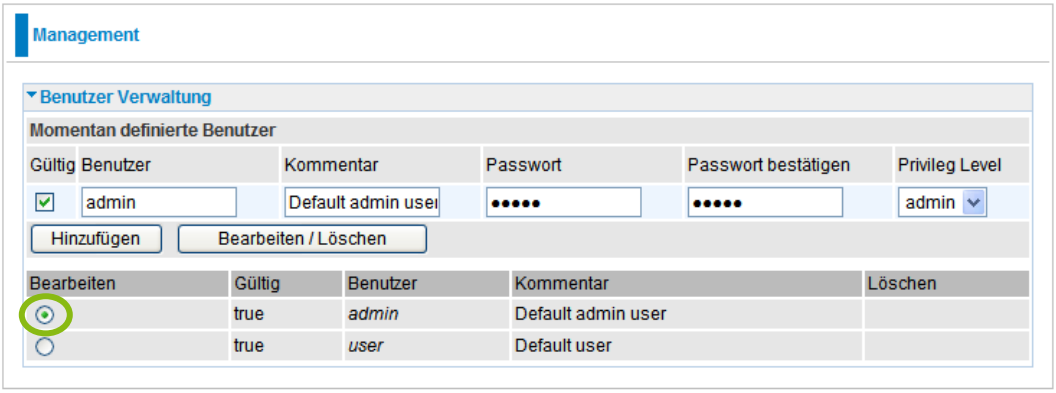
Auf dieser Seite können Sie die Passwörter der Standardkonten „user“/ “admin“ ändern.



Um unerlaubten Zugriff auf Ihr Gerät und dessen Konfiguration zu verhindern, muss jedem Benutzer ein Passwort zugewiesen werden. Sie können mehrere Benutzerkonten einrichten, jedes jeweils mit einem eigenen Passwort.
Sie können bestehende Benutzer bearbeiten und Sie können neue Benutzer hinzufügen, welche wiederum in der Lage sind, Gerätekonfigurationen vorzunehmen.

5.6.1.1 Ändern des Passwortes

Sobald Sie auf den **Bearbeiten Radio Button** geklickt haben, sehen Sie die folgenden Optionen:

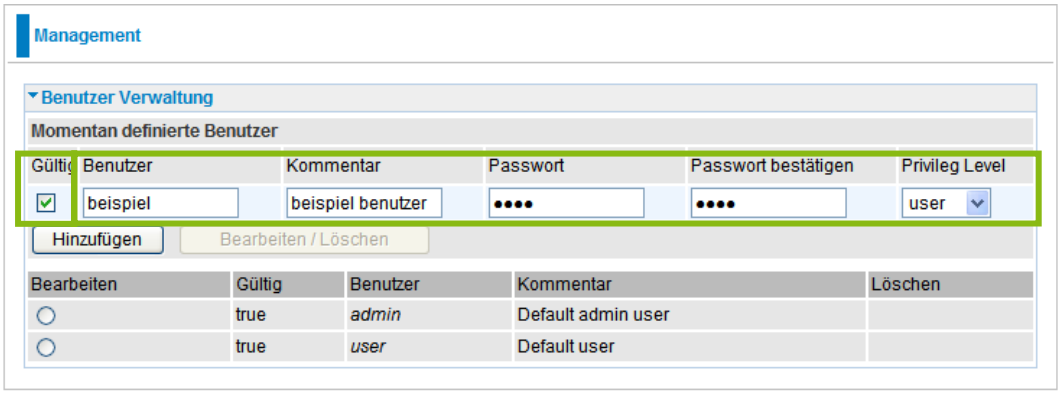


Sie können das **Passwort** des Benutzers ändern, sofern das Konto aktiv und **gültig** ist, sowie auch Kommentare zu jedem Benutzerkonto hinzufügen. Klicken Sie **Bearbeiten/Löschen**, um Ihre Änderungen zu speichern. Sie können die Standardkonten „user“/ „admin“ nicht löschen. Jedoch können Sie jedes neu erstellte Konto löschen, indem Sie **Bearbeiten/Löschen** bei selektiertem **Löschen Radio Button** klicken. Es wird empfohlen, dass Standardpasswort vom „**user**“ Standardkonto bei Erhalt des Gerätes sofort zu ändern. Sowie wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird.

© Internetagentur Schott GmbH, 2010. All rights reserved.

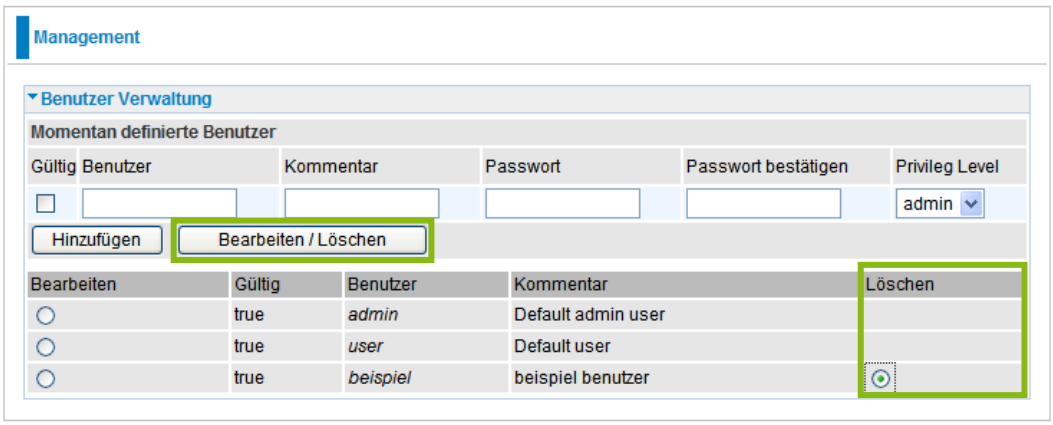
5.6.1.2 Ein Benutzerkonto erstellen

Wenn Sie ein Benutzerkonto erstellen, setzen Sie ein Häkchen bei Gültig und füllen Sie die Felder Benutzer, Kommentar, Passwort, und Passwort bestätigen aus. Danach klicken Sie auf **Hinzufügen**, um Ihr neues Konto zu erstellen.



5.6.1.3 Ein Benutzerkonto löschen

Um ein Benutzerkonto zu löschen, klicken Sie den **Löschen Radio Button** und danach auf **Bearbeiten/Löschen**.

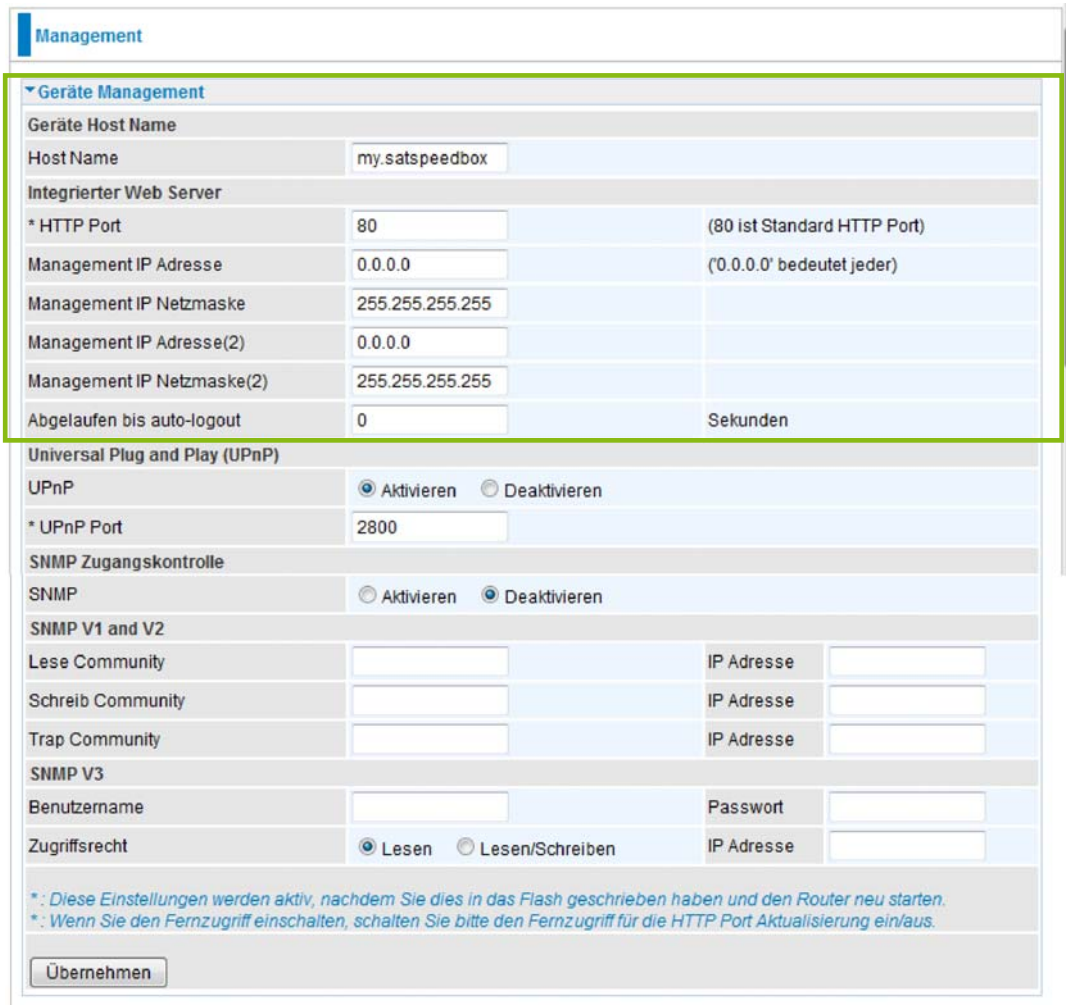


© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.2. Management Kontrolle (Experten)

5.6.2.1 Lokaler Zugriff

Diese Funktion erlaubt es Ihnen, die Sicherheitsoptionen und Überwachung Ihres Gerätes zu kontrollieren.



Geräte Host Name

Host Name	Geben Sie Ihrem Gerät einen Namen, um darauf zuzugreifen. Der Host Name kann nicht aus einem einzigen Wort bestehen. Er setzt sich immer aus zwei Wörtern zusammen, verbunden mit einem '**.**'. Beispiel: Host Name: mysatspeed → Inkorrekt Host Name: my.satspeedbox → Korrekt

Integrierter Web Server

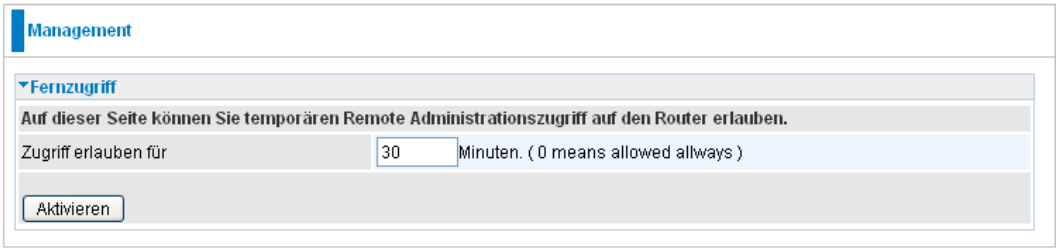
HTTP Port	Dies ist die Portnummer, welche der im Gerät integrierte Webserver braucht (für webbassierte Konfiguration). Der Standardwert ist der Standard http Port 80. Benutzer können einen alternativen Port definieren, beispielsweise, weil sie in ihrem LAN einen Webserver auf einem PC installiert haben.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Management IP Adresse	Sie können einer bestimmten IP Adresse erlauben, auf das Web-GUI Ihres Gerätes einzuloggen. Die IP Adresse 0.0.0.0 schaltet alle IP Adressrestriktionen aus, bedeutet, dass Benutzer von beliebigen IP Adressen einloggen können.
Abgelaufen bis auto-logout	Spezifizieren Sie einen Zeitrahmen, um ein inaktive Sitzung des Benutzers automatisch zu beenden (auto-logout).

Zum Beispiel: Benutzer A wechselt die HTTP Port Nummer auf **100**, setzt seine IP Adresse auf **192.168.100.55** und setzt die logout Zeit auf 300 Sekunden. Folglich wird das Gerät nur User A Zugriff von der IP Adresse **192.168.100.55** für einen Login auf das Web-GUI geben, wenn dieser folgendes in seinem Browser eingibt: http://**192.168.100.1:100**. Nach 300 Sekunden Inaktivität wird das Gerät den User A automatisch ausloggen.

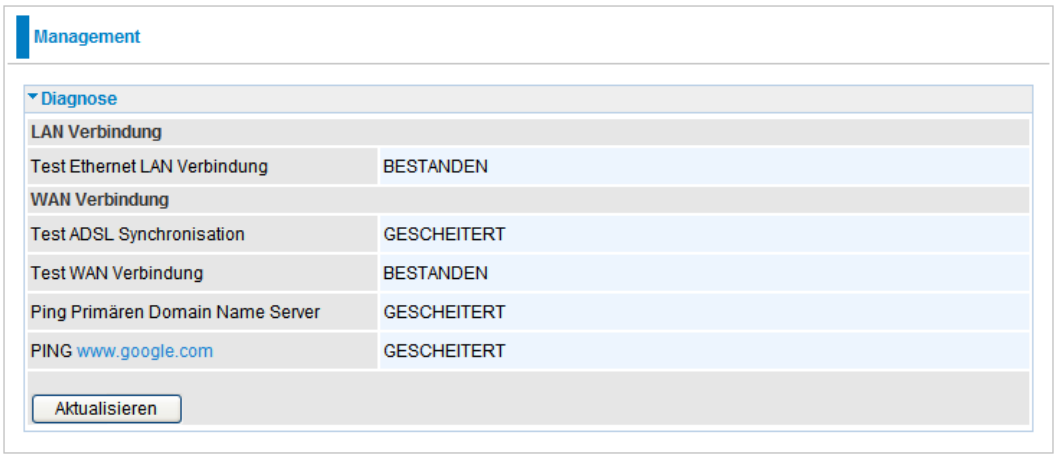
5.6.2.2 Fernzugriff



Um temporär Fernadministration des Gerätes zu erlauben (z.B. von ausserhalb Ihres LAN), wählen Sie eine Zeitdauer und klicken Sie **Aktivieren**.
Wenn Sie permanenten Fernzugriff erlauben möchten, tragen Sie 0 Minuten ein.

5.6.3. Diagnose

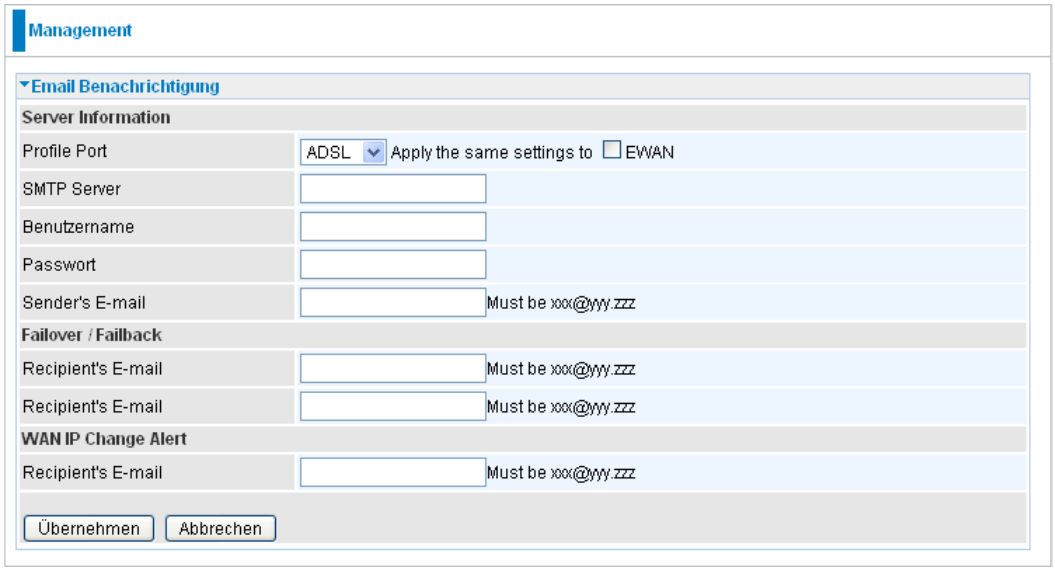
Diese Seite testet die Verbindung zu dem/den Computer/n via Ethernet Ports und ebenfalls die Internetverbindung. Wenn neben **PING** **www.google.com** mehrfach **GESCHEITERT** steht und der Rest BESTANDEN ist, sollten Sie Ihre DNS Einstellungen überprüfen.



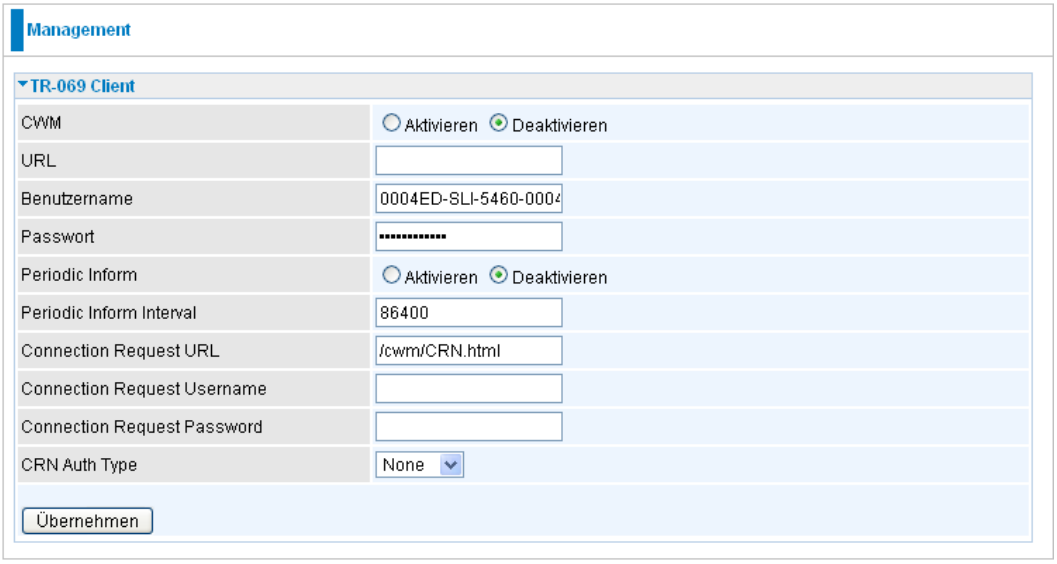
© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.4. Email Benachrichtigung (Experten)

Diese Funktion erlaubt es, automatisch ein Email zu senden, wenn das Gerät auf die Alternativ-Internetverbindung ausweicht (dazu wird auf Kapitel **5.3.2.5 WAN Schnittstelle (Experten)** verwiesen), oder wenn sich die IP Adresse ändert.
Um diese Funktion zu nutzen, geben Sie einen **SMTP Server** ein, auf welchem Sie berechtigt sind Emails zu versenden. Geben Sie Ihre **Email-Adresse, Benutzername** und **Passwort** für diesen Server ein. Tragen Sie ferner die Email-Adresse des Empfängers für die gewünschte Funktion ein.



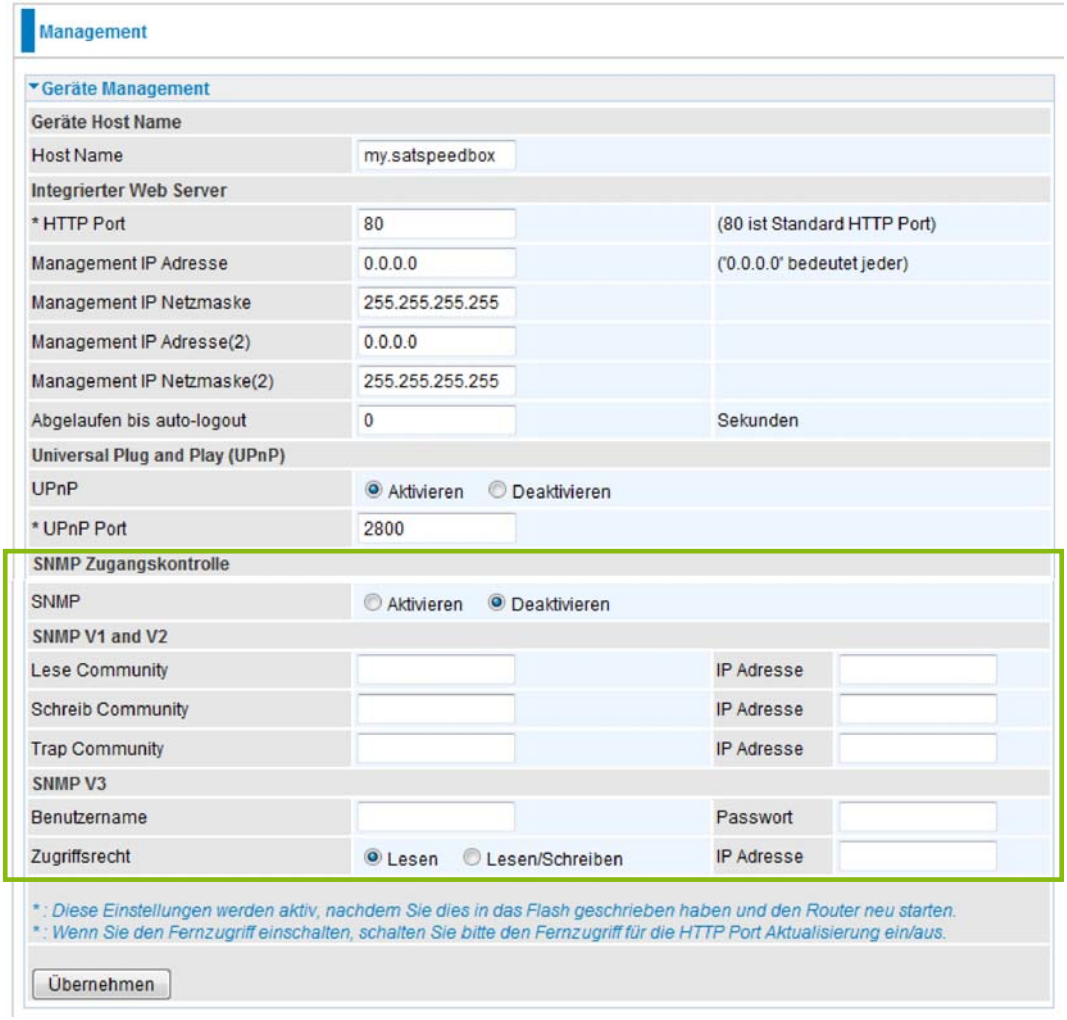
5.6.5. TR-069 Client (Experten)



© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.6. SNMP Agent (Experten)

Diese Feature benötigt zusätzliche Software, die SNMP unterstützt.



SNMP V1 und V2

Lese Community	Spezifiziert einen Namen bestehend aus Lese Community und IP Adresse. Dieser Community Text wird mit dem Community Text in der Konfigurationsdatei verglichen. Wenn die Texte übereinstimmen, bezieht der Benutzer diese IP Adresse und ist befähigt die Daten anzuschauen.
Schreib Community	Spezifiziert einen Namen bestehend aus Schreib Community und IP Adresse. Dieser Community Text wird mit dem Community Text in der Konfigurationsdatei verglichen. Wenn die Texte übereinstimmen, können Benutzer dieser IP Adresse Daten schreiben und lesen.
Trap Community	Spezifiziert einen Namen bestehend aus Trap Community und IP Adresse. Dieser Community Text wird mit dem Community Text in der Konfigurationsdatei verglichen. Wenn die Texte übereinstimmen, werden Benutzer dieser IP Adresse SNMP Traps geschickt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

SNMP V3:

Benutzername / Passwort	Spezifizieren Sie einen Namen und Passwort für die Authentifizierung.
Zugriffsrecht / IP Adresse	Definiert das Zugriffsrecht einer identifizierten IP Adresse. Sobald die Authentifizierung erfolgreich war, können Benutzer dieser IP Adresse Daten schreiben und lesen.

5.6.6.1 Zusätzliche Erklärungen

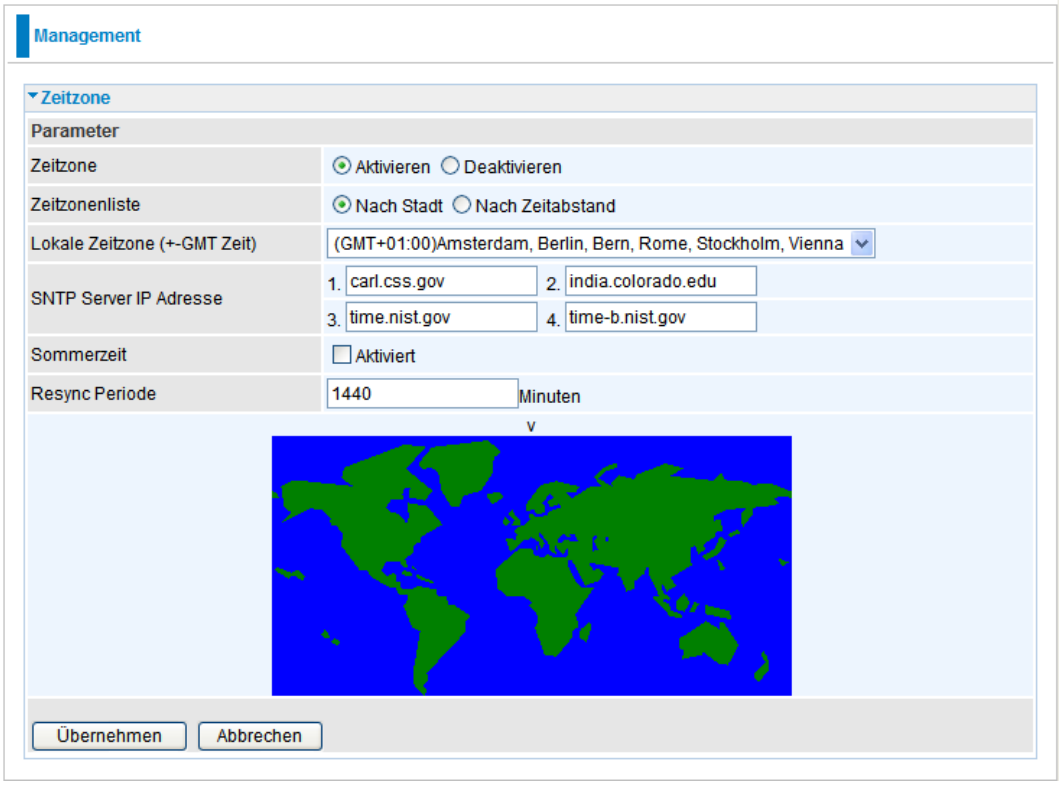
SNMP Version: SNMPv2c und SNMPv3
SNMPv2c ist die Kombination aus den verbesserten Protokoll Features von SNMPv2 ohne die SNMPv2 Sicherheit. Das „c“ leitet sich aus der Tatsache ab, dass SNMPv2c das SNMPv1 Community Text Paradigma für „Sicherheit“ benutzt, aber es wird meist als SNMPv2 Standard akzeptiert.
SNMPv3 ist ein starker Authentifizierungsmechanismus, Authorisierung mit feiner Granulatität für Fernüberwachung.
Unterstützung von Traps: Kaltstart, Fehlschlagen von Authentifizierungen.
Die folgenden MIBs werden unterstützt:

Supported MIBs from	**Detailed**	
	Supported	**Not Supported**
RFC 1213 (MIB-II)	System group Interfaces group Address Translation group IP group ICMP group TCP group UDP group Transmission SNMP group	EGP (not applicable)
RFC 1650 (EtherLike-MIB)	dot3Stats	
RFC 1493 (Bridge MIB)	dot1dBase group dot1dTp group dot1dStp group (if configured as spanning tree)	
RFC 1471 (PPP/LCP MIB)	pppLink group	pppLqr group (not applicable)
RFC 1472 (PPP/Security MIB)	PPP Security Group	
RFC 1473 (PPP/IP MIB)	PPP IP Group	
RFC 1474 (PPP/Bridge MIB)	PPP Bridge Group	
RFC 1573 (IfMIB)	ifMIBObjects Group	
RFC 1695 (atmMIB)	atmMIBObjects	
RFC 1907 (SNMPv2)	only snmpSetSerialNo OID	

Table 4 Supported MIBs

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.7. Internetzeit



Das Gerät hat keine Echtzeit-Uhr integriert; stattdessen benutzt es das Simple Network Time Protocol (SNTP), um die aktuelle Uhrzeit von einem SNTP Server ausserhalb des Netzwerkes zu holen.
Wählen Sie ihre lokale Zeitzone, klicken Sie **Aktivieren** und danach **Übernehmen**. Nach einer erfolgreichen Verbindung zum Internet, wird das Gerät die korrekte lokale Zeit vom spezifizierten SNTP Server erhalten. Wenn Sie einen bestimmten nicht in der Liste aufgeführten Server einstellen möchten, können Sie einfach seine IP Adresse oder seinen Domänennamen eingeben. Ihr ISP bietet evtl. ebenfalls einen SNTP Server.

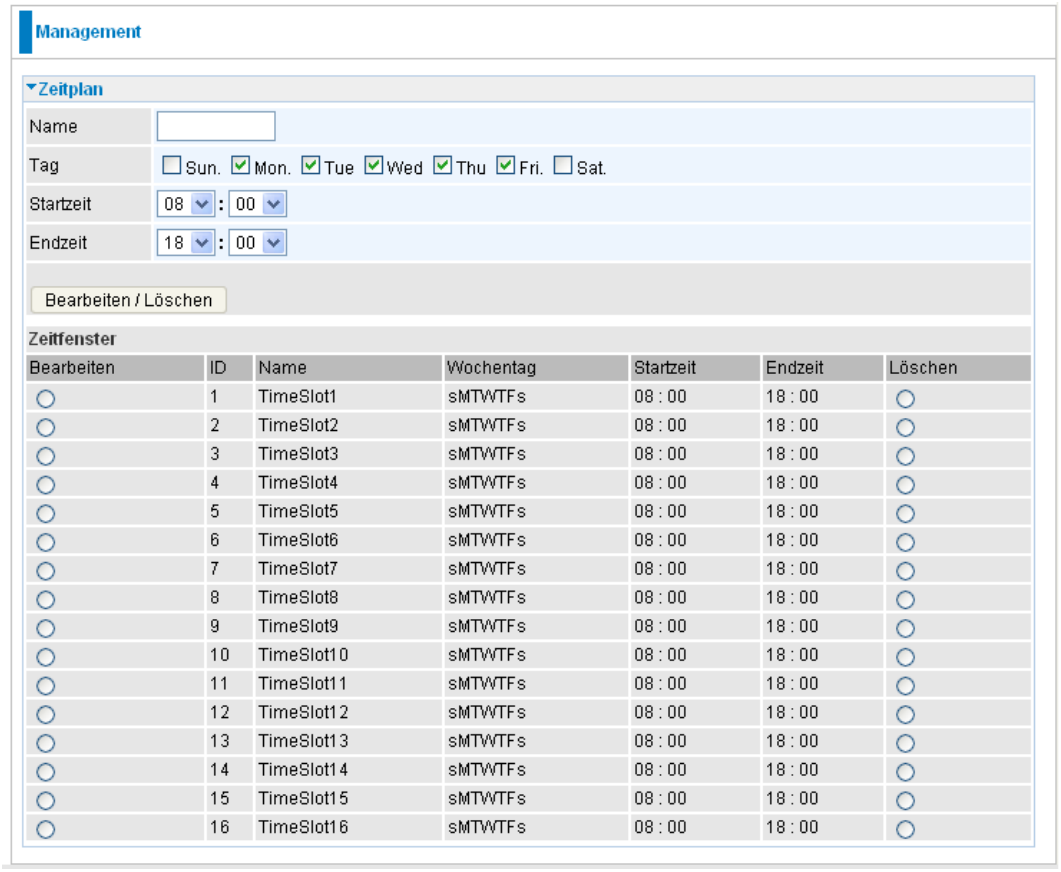
Klicken Sie die **Aktiviert** Checkbox bei der Sommerzeit, wenn Sie Sommerzeit berücksichtigen wollen.

Resync Periode (in Minuten) ist das periodische Intervall, das das Gerät wartet bevor es seine Zeit wieder mit dem angegebenen SNTP Server synchronisiert. Um unnötig hohe Last auf dem SNTP Server zu vermeiden, sollten Sie einen möglichst hohen Intervallwert eingeben.

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.8. Zeitplan

Der Zeitplan unterstützt bis zu 16 Zeitfenster, welche Sie für verschiedene Applikationen des Gerätes benutzen können (z.B. Port Forwarding). In jedem Zeitfenster können Sie verschiedene Tage spezifizieren (beispielsweise Montag bis Sonntag), an welchen Sie den Internetzugriff von Benutzern oder Applikationen erlauben oder verbieten.


Management
Zeitplan
Name
Tag
Sun. Mon. Tue Wed Thu Fri. Sat.
Startzeit
08 : 00
Endzeit
18 : 00
Bearbeiten / Löschen
Zeitfenster
Bearbeiten ID Name Wochentag Startzeit Endzeit Löschen
1 TimeSlot1 sMTWTFs 08 : 00 18 : 00
2 TimeSlot2 sMTWTFs 08 : 00 18 : 00
3 TimeSlot3 sMTWTFs 08 : 00 18 : 00
4 TimeSlot4 sMTWTFs 08 : 00 18 : 00
5 TimeSlot5 sMTWTFs 08 : 00 18 : 00
6 TimeSlot6 sMTWTFs 08 : 00 18 : 00
7 TimeSlot7 sMTWTFs 08 : 00 18 : 00
8 TimeSlot8 sMTWTFs 08 : 00 18 : 00
9 TimeSlot9 sMTWTFs 08 : 00 18 : 00
10 TimeSlot10 sMTWTFs 08 : 00 18 : 00
11 TimeSlot11 sMTWTFs 08 : 00 18 : 00
12 TimeSlot12 sMTWTFs 08 : 00 18 : 00
13 TimeSlot13 sMTWTFs 08 : 00 18 : 00
14 TimeSlot14 sMTWTFs 08 : 00 18 : 00
15 TimeSlot15 sMTWTFs 08 : 00 18 : 00
16 TimeSlot16 sMTWTFs 08 : 00 18 : 00

ID	Das ist der Index des jeweiligen Zeitfensters.
Name	Eine benutzerdefinierte Beschreibung zur Identifizierung dieses Zeitfensters.
Wochentag	Voreingestellt ist von Montag bis Freitag. Wählen Sie die Tage, zu welchen das Zeitfenster aktiv sein soll.
Startzeit	Voreingestellt ist 8 Uhr. Wählen Sie die Startzeit im Zeitplan.
Endzeit	Voreingestellt ist 18 Uhr. Wählen Sie die Endzeit im Zeitplan.

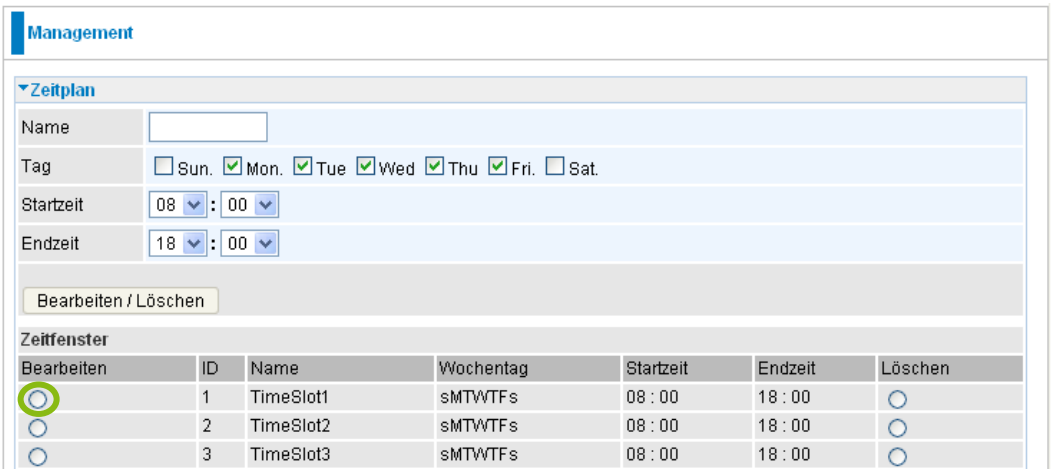
Klicken Sie auf **Bearbeiten/Löschen**, um Ihre Änderungen zu übernehmen.

Ein Zeitfenster löschen
Wählen Sie den Löschen Radio Button und klicken Sie auf **Bearbeiten/Löschen**, um das selektierte Zeitfenster zu löschen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

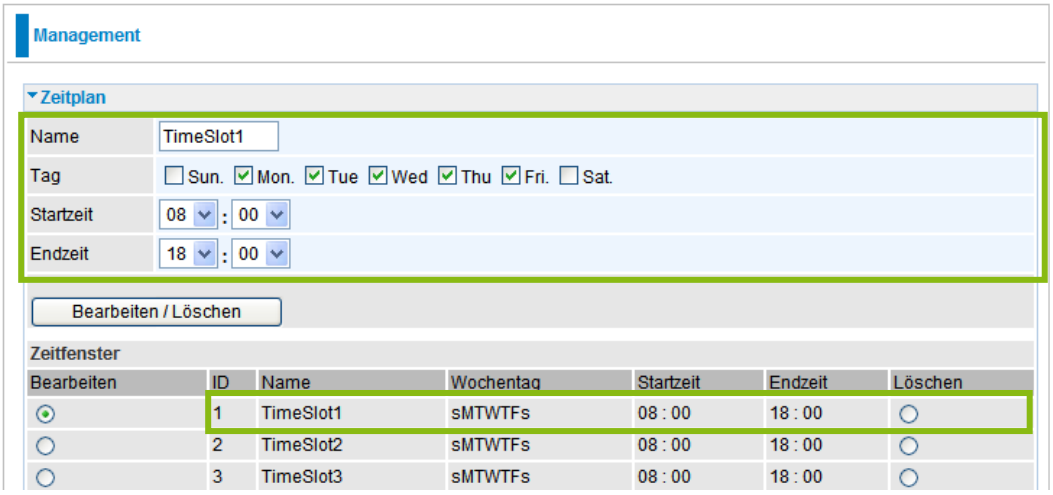
5.6.8.1 Beispiel: Ein Zeitfenster bearbeiten

1. Wählen Sie ein Zeitfenster (ID 1 bis ID 16) und klicken Sie den **Bearbeiten** Radio Button.



Bemerkung: Grossbuchstaben repräsentieren die selektieren Tage, während Kleinbuchstaben Tage ohne angewendete Regel zeigen.

2. Wenn Sie auf den **Bearbeiten** Radio Button klicken, werden die detaillierten Einstellungen dieses Zeitfensters angezeigt.

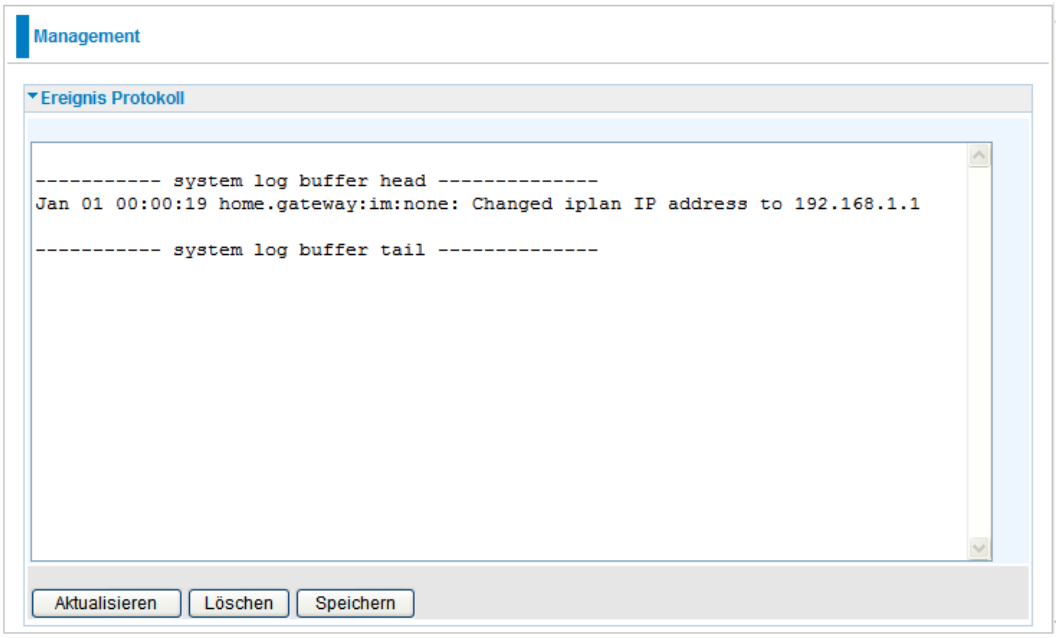


© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.9. System Log (Experten)

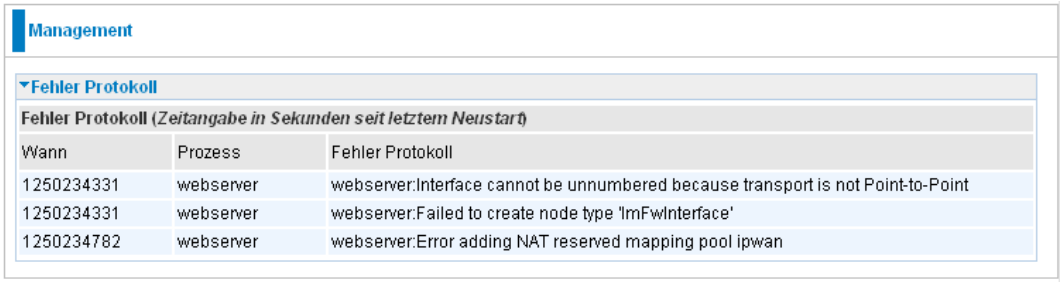
5.6.9.1 Ereignis Protokoll

Diese Seite zeigt die Ereignis Protokoll Einträge des Gerätes. Wichtige Einträge werden in dieses Fenster geschrieben, wie zum Beispiel, wenn die ADSL Leitung nicht verbunden ist oder auch Firewall Ereignisse, die bei eingeschalteter „Intrusion or Blocking“ Regel erscheinen.



5.6.9.2 Fehler Protokoll

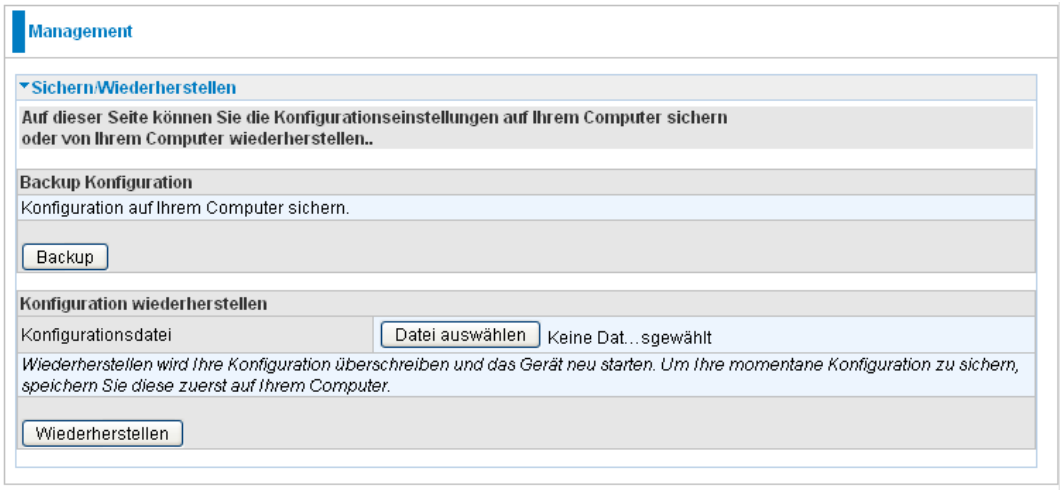
Jeder Fehler, der das Gerät betrifft (z.B. Falscheingaben bei Einträgen) wird hier angezeigt.



5.6.10. Backup Konfiguration

Diese Funktion erlaubt Ihnen, die aktuelle Konfiguration in einer Datei auf Ihrem PC zu speichern oder eine zuvor gespeicherte Konfiguration zu laden. Dies ist hilfreich, wenn Sie mit verschiedenen Einstellungen experimentieren wollen, im Wissen, dass Sie im Fehlerfall ein Backup haben. Es empfiehlt, sich ein Backup der Geräteeinstellungen zu machen, bevor man signifikante Konfigurationsänderungen am Gerät vornimmt.

© Internetagentur Schott GmbH, 2010. All rights reserved.

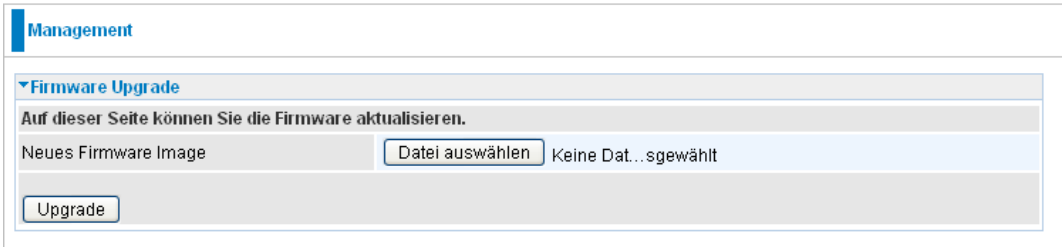

Management
Sichern/Wiederherstellen
Auf dieser Seite können Sie die Konfigurationseinstellungen auf Ihrem Computer sichern oder von Ihrem Computer wiederherstellen..
Backup Konfiguration
Konfiguration auf Ihrem Computer sichern.
Backup
Konfiguration wiederherstellen
Konfigurationsdatei
Datei auswählen
Keine Dat...sgewählt
Wiederherstellen wird Ihre Konfiguration überschreiben und das Gerät neu starten. Um Ihre momentane Konfiguration zu sichern, speichern Sie diese zuerst auf Ihrem Computer.
Wiederherstellen

Drücken Sie auf **Backup**, um den Speicherzielort der Konfigurationsdatei zu wählen. Hier können Sie auch den Dateinamen verändern, wenn Sie mehrere Backups speichern wollen.
Drücken Sie auf **Datei auswählen**, um eine Datei von Ihrem Computer zu laden. Sie sollten nur Konfigurationsdateien verwenden, die von der Backup Funktion **mit der gleichen Firmwareversion** generiert worden sind.

Vorsicht	**Konfigurationsdateien auf Ihrem Computer dürfen in keinem Fall manuell bearbeitet werden.**

Nach der Auswahl der Konfigurationsdatei drücken Sie auf **Wiederherstellen**, um die Konfiguration in Ihr Gerät zu laden.

5.6.11. Firmware Upgrade



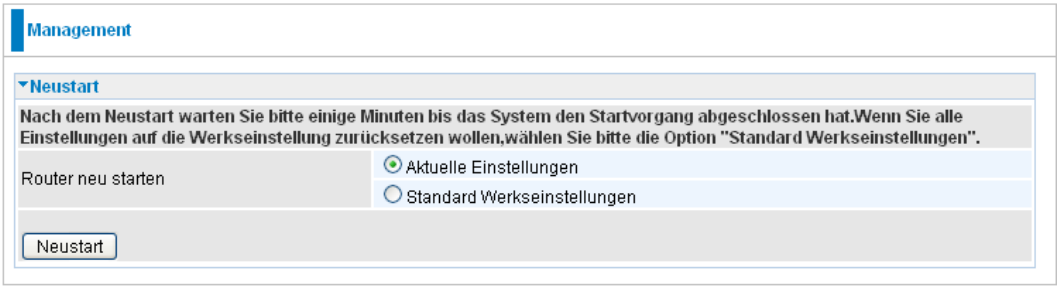
Klicken Sie auf **Datei auswählen**, um ein neues Firmware Image, das sich auf Ihrem Computer befindet, auszuwählen. Klicken Sie auf **Upgrade**, um die neue Firmware auf Ihr Gerät zu laden.

Hinweis	**Unterbrechen Sie NICHT die Stromversorgung oder den Upgrade Vorgang, solange dieser noch läuft.** **Unsachgemässe Eingriffe könne das Gerät beschädigen.**

© Internetagentur Schott GmbH, 2010. All rights reserved.

5.6.12. Neustart

Klicken Sie auf **Neustart** mit der Option **Aktuelle Einstellungen**, um Ihr Gerät neu zu starten (mit der zuletzt gespeicherten Konfiguration)

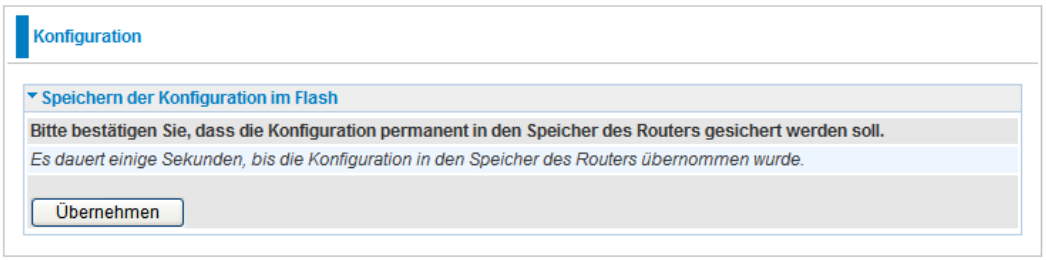

Management
Neustart
Nach dem Neustart warten Sie bitte einige Minuten bis das System den Startvorgang abgeschlossen hat.Wenn Sie alle Einstellungen auf die Werkseinstellung zurücksetzen wollen,wählen Sie bitte die Option "Standard Werkseinstellungen".
Router neu starten
Aktuelle Einstellungen
Standard Werkseinstellungen
Neustart

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten (z.B. nach einem Firmware Upgrade oder wenn Sie eine inkorrekte Konfiguration gespeichert haben), wählen Sie die Option **Standard Werkseinstellungen**.

Sie können ihr Gerät auch auf die Werkseinstellungen zurücksetzen, indem Sie den kleinen Knopf im Gehäuse auf der Hinterseite für mehr als 6 Sekunden gedrückt halten. Anschliessend müssen Sie das Gerät mithilfe des Netzschalters aus- und einschalten.

5.7. Konfiguration speichern

Wenn Sie Konfigurationsänderungen machen, werden diese nur temporär gespeichert und bei einem Neustart des Gerätes wieder verworfen. Um die Konfiguration dauerhaft zu speichern, klicken Sie auf **Konfiguration speichern** am unteren Ende der Seite. Danach erscheint folgendes Fenster:


Konfiguration
Speichern der Konfiguration im Flash
Bitte bestätigen Sie, dass die Konfiguration permanent in den Speicher des Routers gesichert werden soll.
Es dauert einige Sekunden, bis die Konfiguration in den Speicher des Routers übernommen wurde.
Übernehmen

Klicken Sie auf **Übernehmen**, um die Konfiguration zu speichern.

5.8. Abmelden

Um das Webinterface des Gerätes zu verlassen, klicken Sie auf **Abmelden** am unteren Ende der Seite. Stellen Sie sicher, dass Sie davor Ihre Konfigurationsänderungen gespeichert haben.
Seien Sie sich bewusst, dass der Zugriff via Webinterface auf einen Benutzer beschränkt ist. Sobald sich ein Computer angemeldet hat, können andere nicht zugreifen, bis sich ersterer wieder abmeldet. Wenn der vorherige Computer vergessen hat sich abzumelden, dann kann der nachfolgende nach einer benutzerdefinierten Zeit Zugriff erhalten. Voreingestellt sind 5 Minuten. Sie können diesen Wert ändern, dazu wird auf Kapitel **5.6.2.1 Lokaler Zugriff** verwiesen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

6. Anhang

6.1. Werkseinstellungen

Um das Gerät auf die Werkseinstellungen zurückzusetzen, drücken Sie den mit „**Reset**“ beschrifteten Knopf auf der Hinterseite des Gerätes, bis alle LEDs leuchten. Danach müssen Sie das Gerät mittels Netzschalter aus- und wieder einschalten.
Sobald das Gerät neu gestartet ist, kann es via Webbrowser über die Adresse **192.168.100.1** erreicht werden.
Alle Ihre Einstellungen gehen bei einer Rücksetzung auf Werkseinstellung verloren. Benutzen sie daher “**user**” als Benutzername und “**user**” als Passwort, um einzuloggen. Gegebenenfalls müssen Sie Ihre IP Adresseinstellungen an Ihrem Computer zurücksetzen.

6.2. Zugriff auf die Weboberfläche

Management Adresse	My.satspeedbox	
Management Adresse	192.168.100.1	
Benutzername	user	admin
Passwort	user	admin

6.3. Anleitung für Zusatzdienste

Telefonfunktionen (z.B. Aktivierung, Deaktivierung, Funktionskonfigurationen,…) können mittels Telefontastatur benutzt werden. Die folgende Tabelle fasst die entsprechenden Tastencodes zusammen.

00#	Benutzung des PSTN anstelle von VoIP.
R 2	Zwischen zwei Anrufen umschalten.
R 3	Verbindung zweier Anrufe, zum Aufbau einer Konferenzschaltung.
<Nummer> #	Ausgehenden Anruf sofort tätigen (Wählzeitüberschreitung ignorieren)
##	Wahlwiederholung
X#	Benutzung von Schnellwahl
***67**	Rufnummerunterdrückung
***69**	Rückruf
***20**	Aktivieren der Funktion „Bitte nicht stören“
***80**	Deaktivieren der Frunktion „Bitte nicht stören“
***90 <Nummer>**	Rufweiterleitung
***74<x><Nummer>#**	Definition einer Schnellwahlnummer

Bemerkung: R heisst Hook flash.

© Internetagentur Schott GmbH, 2010. All rights reserved.

7. Fehlerbehebung

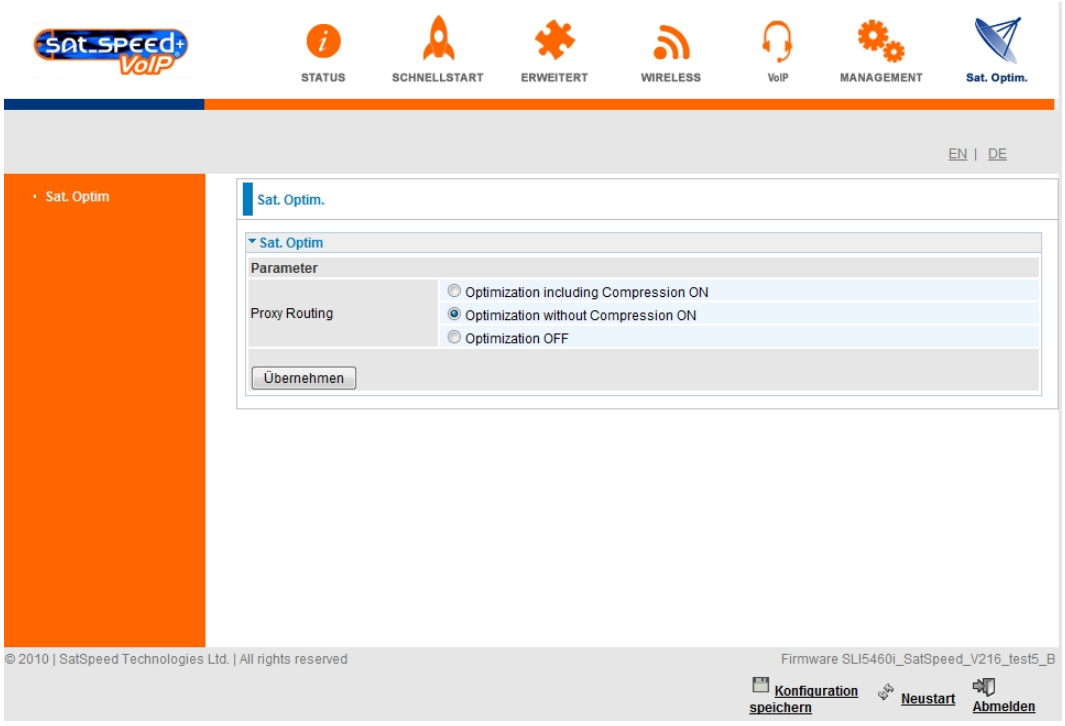
1. Keine LEDs leuchten, wenn Sie das IAD einschalten.
Kontrollieren Sie die Verbindung zwischen dem Steckernetzteil und dem IAD. Sollte der Fehler weiterhin bestehen, liegt gegebenenfalls ein Hardwareproblem vor. In diesem Fall sollten Sie den technischen Support kontaktieren.

2. Sie haben Ihr Benutzername / Passwort zum IAD vergessen.
Versuchen Sie sich mit dem Standard-Benutzernamen /-Passwort anzumelden. Diese Angaben finden Sie im Benutzerhandbuch. Sollte dies nicht funktionieren, setzen Sie das IAD auf Werkseinstellungen zurück, indem Sie auf der Geräterückseite den Reset-Knopf für 6 Sekunden oder etwas länger, betätigen.

3. Sie können keine anderen Computer im LAN erreichen.
Kontrollieren Sie die Ethernet LEDs auf der Gerätevorderseite. Es sollten die LEDs leuchten, an welchen auf der Rückseite ein aktiver Computer verbunden ist.
Sollte dies nicht übereinstimmen, kontrollieren Sie die Kabelverbindung zwischen dem IAD und dem entsprechenden Computer. Stellen Sie sicher, dass das Problem nicht von einer Software-Firewall verursacht wird. Ausserdem sollten Sie sicherstellen, dass die Computer sich in demselben Netzwerk wie das IAD befinden. Dazu müssen Sie die IP Adressen kontrollieren (jeder Computer muss eine eigene IP Adresse besitzen) und Subnetmasken (muss überall dieselbe sein).

4. Häufiger Verlust der ADSL Verbindung.
Stellen Sie sicher, dass alle anderen Geräte an der Telefonleitung (z.B. Telefone, Faxgeräte, usw.) durch ein Splitter/Filter vom IAD „getrennt“. Stellen Sie sicher, dass die Splitter / Filter korrekt installiert wurden. Sollten Sie über eine Alarmanlage mit Telefonverbindung verfügen, stellen Sie sicher, dass diese keine Probleme verursacht. Behebt dies das Problem nicht, wenden Sie sich an den technischen Support.

8. Internet via Satellite Optimierung



© Internetagentur Schott GmbH, 2010. All rights reserved.

Diese Funktion ist ausschließlich via “satspeed NEXT Generation Gateways”, verfügbar. Bitte kontaktieren Sie Ihren Internet Service Provider ob dieser diese Funktion bereitstellt. Es gibt 3 Einstell-Möglichkeiten:

1. **Optimization including compression ON**
   → (http, https und ftp Traffic wird zum satspeed NEXT Generation Gateway weitergeleitet. Der Traffic wird komprimiert sowie speziell für Internet via Satellit optimiert).
2. **Optimization without compression ON**
   → (http, https und ftp Traffic wird zum satspeed NEXT Generation Gateway weitergeleitet. Der Traffic wird jedoch NICHTkomprimiert aber trotzdem speziell für Internet via Satellit optimiert).
3. **Optimization OFF**
   → (http, https und ftp Traffic wird NICHT zum satspeed NEXT Generation Gateway weitergeleitet. Der Traffic wird somit NICHTkomprimiert und für Internet via Satellit optimiert).

© Internetagentur Schott GmbH, 2010. All rights reserved.

Copyright und Lizenzen

Mac OS is a registered Trademark of Apple Computer, Inc.
Windows 2000, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

9.1 GNU GPL – General Public License

Dieses Produkt benutzt keine GNU GPL-Quellen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

10. Glossar

100Base-T	Auch bekannt als Fast Ethernet; ein Standard für Ethernet Kabel mit einer Datenübertragung von bis zu 100 Mbps.
10Base-T	Ein älterer Standard für Ethernet Kabel mit einer Datenübertragungsrate von bis zu 10 Mbps.
802.11b, 802.11g	Eine Familie von Spezifikationen für wireless Netzwerke definiert durch IEEE (Institute of Electrical and Electronics Engineers). Beinhaltet den 802.11b Standard, der high-speed (bis zu 11 Mbps) wireless Datenübertragung unterstützt.
Access Point	Ein Gerät, das Daten zwischen verschiedenen Computern eines Netzwerkes austauscht. Ein Access Point hat typischerweise keine Firewall oder NAT Möglichkeiten.
Ad hoc Netzwerk	Ein allein stehendes Computer-zu-Computer Netzwerk. Anders als ein fest installiertes Netzwerk, hat ein ad hoc Netzwerk keinen Gateway Router.
Adapter	Auch bekannt als Netzwerk Interface Karte (NIC = network interface card). Eine Erweiterungskarte oder ein anderes Gerät, welche einem Computer, einem Drucker oder anderem Gerät Zugang zum Netzwerk gewährt.
Administrator	Eine Person, die verantwortlich ist für das Planen, Konfigurieren und Verwalten des alltäglichen Arbeitsablaufs des Computernetzwerkes. Die Aufgaben eines Administrators umfassen das Installieren neuer Arbeitsplätze und anderer Geräte, das Hinzufügen und Entfernen von Personen auf der Liste der autorisierten Benutzer, das Archivieren von Dateien, das Überwachen des Passwortschutzes und anderer Sicherheits-massnahmen, das Beobachten des Gebrauchs von gemeinsamen Ressourcen und die Bearbeitung von nicht funktionierenden Geräten.
Authentifi-zierung	Der Prozess ein Individuum zu identifizieren, normalerweise basierend auf einem Benutzername und einem Passwort. In einem Sicherheitssystem unterscheidet sich die Authentifizierung von der Autorisierung. Autorisierung ist der Prozess einem Einzelnen aufgrund seiner Identität Zugang zu Systemobjekten zu gewähren. Authentifizierung stellt nur sicher, dass ein Individuum auch das ist, was es vorgibt zu sein. Aber es sagt nicht aus über die Zugriffsrechte des Individuums.
Bandbreite	Die Menge von Informationen oder die Grösse einer Datei, die auf einmal über eine Netzwerkverbindung gesendet werden kann. Eine Verbindung mit mehr Bandbreite kann die Information schneller übertragen.
Breitband Verbindung	Eine high-speed Verbindung, typischerweise 256 Kbps oder schneller. Breitband Dienste umfassen Kabel Modems und DSL.
Breitband Modem	Ein Gerät, das eine Breitband Verbindung für den Zugang zum Internet ermöglicht. Die zwei gebräuchlichsten Typen von Breitband Modems sind Kabel Modems, die auf der Infrastruktur des Kabelfernsehens basieren, und DSL Modems, die auf den Telefonleitungen, die mit DSL Geschwindigkeit operieren, basieren.
Bridge	Ein Gerät, das Informationspakete von einem Abschnitt eines Netzwerkes zu einem anderen übermittelt. Eine Bridge übermittelt nur die Pakete, die für die Kommunikation zwischen den Segmenten notwendig ist.
Broadcast	Broadcast sendet eine Nachricht an alle Clients in einem Netzwerk, wohingegen Multicast eine Nachricht nur an eine ausgewählte Gruppe von Empfängern schickt.
Bus	Ein Set von Hardware Leitungen, die für die Datenübertragung unter den Komponenten eines Computer-Systems verwendet werden. Ein Bus ermöglicht im Wesentlichen, dass verschiedene Teile des Systems Daten gemeinsam nützen können. Ein Bus verbindet zum Beispiel die Steuerung des Laufwerks, den Speicher und die Input/Output Ports zum Mikroprozessor.

© Internetagentur Schott GmbH, 2010. All rights reserved.

CHAP	Ist die Abkürzung für “challenge handshake authentication protocol“. Dies Ist eine Art der Authentifizierung bei dem der Authentifizierungsagent (typischerweise ein Netzwerk-Server) einen zufälligen Wert (Challenge), der nur einmal verwendet wird, an den Client schickt. Der Client berechnet aus diesem Wert und dem zuvor definierten Passwort einen neuen Wert, den der Client an den Server zurück schickt.
Client	Jeder Computer, der sich mit dem Netzwerk verbindet oder jedes Programm, das einen Dienst von einem anderen Computer des Netzwerkes anfordert. Für lokale Netzwerke oder das Internet ist ein Client ein Computer, der die von einem Server bereitgestellten gemeinsam benutzten Netzwerk Ressourcen verwendet.
Client/Server Netzwerk	Ein Netzwerk von zwei oder mehreren Computern, das auf einen zentralen Server angewiesen ist, um die Verbindungen zu vermitteln oder zusätzliche System Ressourcen anzubieten. Diese Abhängigkeit von einem Server unterscheidet ein Client/Server Netzwerk von einem Peer-to-Peer Netzwerk.
Computername	Ein Name, der einen Computer in einem Netzwerk eindeutig identifiziert, sodass alle seine gemeinsam benutzen Ressourcen für andere Computer des Netzwerkes zugänglich sind. Ein Computername kann nicht derselbe sein, wie irgendein anderer Computername oder Domain Name im Netzwerk.
DHCP	Abkürzung für “dynamic host configuration protocol“. Ein TCP/IP Protokoll, das automatisch temporäre IP-Adressen an Computer im lokalen Netzwerk (LAN) zuweisst. Das IAD unterstützt die Verwendung von DHCP. Sie können DHCP verwenden, um eine Internetverbindung mit mehreren Computern im Netzwerk gemeinsam zu nutzen.
DMZ	Abkürzung für “demilitarized zone“ (demilitarisierte Zone). Eine Ansammlung von Geräten und Subnetzen, die zwischen einem privaten Netzwerk und dem Internet platziert sind. Dies hilft das private Netzwerk vor nicht autorisierten Internetbenutzern zu schützen.
DNS	Abkürzung für “domain name system“. Ein Dienst, der hauptsächlich im Internet verwendet wird, um einen Hostnamen in die entsprechende Internet-Adresse zu übersetzen. Die DNS Datenbank bildet DNS Domain Namen in IP-Adressen ab, so dass Benutzer Computer und Dienste über benutzerfreundliche Namen lokalisieren können.
Domain	Eine Ansammlung von Computern in einer vernetzten Computer Umgebung, die eine gemeinsame Domain Datenbank und Sicherheitspolitik haben. Eine Domain wird als Einheit mit gemeinsamen Regeln und Abläufen verwaltet. Jede Domain hat einen eindeutigen Namen.
Domain Name	Eine Adresse einer Netzwerkverbindung, die den Besitzer dieser Adresse in einem hierarchischen Format identifiziert: Server.Organisation.Typ. Zum Beispiel http://www.whitehouse.gov identifiziert den Webserver des Weissen Hauses, welcher ein Teil der US Regierung ist.
DSL	Abkürzung für “digital subscriber line“. Eine konstante, digitale, high-speed Verbindung zum Internet, die Standard Telefondrähte aus Kupfer verwendet.
DSL Modem	Ein Gerät. das eine Breitband Verbindung für den Zugang zum Internet ermöglicht. DSL Modems basieren auf Telefonleitungen, die mit DSL Geschwindigkeit operieren.
Duplex	Ein Verbindungsmodus. Voll-Duplex Übertragung erlaubt die gleichzeitige Informationsübertragung zwischen dem Sender und dem Empfänger. Halb-Dublex Übertragung erlaubt nur eine Datenübertragung in eine Richtung zur selben Zeit.
Durchsatz	Die Datenübertragungsrate eines Netzwerkes, gemessen in Anzahl Kilobytes, die pro Sekunde übertragen werden.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Dynamische IP-Adresse	Die IP-Adresse, die einem Gerät, das die IP-Adresse benötigt, zugewiesen wurde (unter Verwendung eines DHCP Protokolls)).Eine dynamische IP-Adresse kann von einem ISP auch einem Gateway oder einem Router zugewiesen werden.
Einstellungen rücksetzen	Ausdruck, um den Prozess zu beschreiben, wenn die aktuellen Einstellungen Ihres IADs gelöscht werden und die Werkseinstellungen wiederhergestellt werden. Sie erreichen dies, indem Sie den Reset Knopf für länger als 5 Sekunden drücken. Beachten Sie dass dies nicht das Gleiche ist, wie das Neustarten des IADs.
Ethernet	Eine Standard Vernetzung, welche Kabel verwendet, um Zugang zum Netzwerk anzubieten. Ethernet ist die am meisten installierte Technologie, um Computer miteinander zu verbinden.
Firewall	Ein Sicherheitssystem, das hilft ein Netzwerk von externen Bedrohungen zu schützen (Zum Beispiel vor Hacker Angriffen, die von ausserhalb des Netzwerkes her kommen). Eine Hardware Firewall ist ein Gerät für den Netzwerkverkehr, das spezifische Einstellungen zur Datenüberprüfung hat und hilft alle an dieses Gerät angeschlossenen Geräte zu schützen.
Firmware	Software Information, die auf einem permanenten Speicher auf dem Gerät abgelegt ist.
Flash Speicher	Ein Speichertyp, bei dem die Daten nicht verloren gehen, wenn der Strom entfernt wird. Flash Speicher wird üblicherweise als Ergänzung zu, oder als Ersatz für Festplatten in portabeln Computern verwendet. In diesem Zusammenhang ist der Flash Speicher entweder in der Einheit eingebaut, oder mehr verbreitet als PC-Karte erhältlich, die in einen PCMCIA Steckplatz eingesetzt werden kann.
FTP	Abkürzung für “file transfer protocol“. Dies ist das Standard Internet Protokoll, um Dateien herunterzuladen oder von einem Computer auf einen anderen zu verschieben.
Gateway	Ein Gerät, das als zentraler Punkt für vernetzte Geräte agiert, um übertragene Nachrichten zu empfangen und diese weiterzuleiten. Das IAD kann viele Computer zu einem einzelnen Netzwerk verlinken und kann eine verschlüsselte Internetverbindung mit verkabelten und drahtlosen Geräten freigeben.
Gateway Adresse	Die IP-Adresse, die Sie benutzen, wenn Sie eine Verbindung ausserhalb Ihres unmittelbaren Netzwerkes machen.
Gemeinsam benutzter Ordner	Ein Ordner (auf einem Computer), der für andere Personen im Netzwerk zum Gebrauch zur Verfügung steht.
Gemeinsam benutzter Drucker	Ein Drucker (angeschlossen an einen Computer), der für andere Personen im Netzwerk zum Gebrauch zur Verfügung steht.
Gemeinsame Nutzung (Sharing)	Ressourcen, die mit einem Computer verbunden sind, werden Benutzern von anderen Computern des Netzwerkes zur Verfügung gestellt.
Hexadezimal	Ein Zahlensystem, das 16 anstatt 10 als Basis für die Repräsentation der Zahlen verwendet. Es wird daher von einem Basis-16 Zahlensystem gesprochen. Das hexadezimale System verwendet die Ziffern 0 bis 9 und die Buchstaben A bis F um die die dezimalen Zahlen 0 bis 15 darzustellen. Der hexadezimale Buchstabe D repräsentiert zum Beispiel die dezimale Zahl 13. Eine hexadezimale Ziffer ist equivalent zu 4 Bits und ein Byte kann mit 2 hexadezimalen Ziffern ausgedrückt werden.
Hostname	Der DNS Name eine Gerätes in einem Netzwerk. Er wird verwendet, um den Prozess der Lokalisierung eines Computers im Netzwerk zu vereinfachen.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Hub	Ein Gerät, das mehrere Anschlüsse hat und das als zentraler Punkt für die Kommunikationsverbindungen zwischen dem Gerät und dem Netzwerk dient. Wenn Daten an einem Anschluss ankommen, werden diese zu den anderen Anschlüssen kopiert.
Internet Domain	Eine Ansammlung von Computern in einer vernetzten Computer Umgebung, die eine gemeinsame Domain Datenbank und Sicherheitspolitik haben. Eine Domain wird als Einheit mit gemeinsamen Regeln und Abläufen administriert und jede Domain hat einen eindeutigen Namen.
Intranet	Ein Netzwerk innerhalb einer Organisation, das Internettechnologien (wie einen Web-Browser, um Informationen anzuschauen) und Protokolle (wie TCP/IP) verwendet, aber das nur für bestimmte Personen, wie zum Beispiel Angestellte einer Firma, zugänglich ist. Ein Intranet wird auch als privates Netzwerk bezeichnet. Einige Intranets bieten Zugang zum Internet, aber solche Verbindungen werden durch eine Firewall geführt.
IP	Abkürzung für “Internet Protokoll“. Das Protokoll innerhalb TCP/IP, das verwendet wird, um Daten zwischen Computern über das Internet zu senden. Dieses Protokoll regelt das Routing von Daten, die in kleineren Komponenten (Paketen) übertragen werden.
IP-Adresse	Abkürzung für “Internet Protokoll Adresse“. IP ist das Protokoll innerhalb TCP/IP, das verwendet wird, um Daten zwischen Computern über das Internet zu senden. Eine IP-Adresse ist eine zugewiesene Nummer, um einen Computer zu identifizieren, der über TCP/IP mit einem Netzwerk verbunden ist. Eine IP-Adresse besteht aus vier Nummer (wobei keine dieser Nummern grösser als 255 sein kann) getrennt durch Punkte, so wie zum Beispiel 192.168.100.1.
IPsec	Wird verbreitet eingesetzt, um VPNs (Virtuel Private Networks) zu implementieren.
ISP	Abkürzung für “internet service provider“. Eine Firma, die Einzelpersonen oder anderen Firmen Zugang zum Internet anbietet.
Kabel Modem	Ein Gerät. das eine Breitband Verbindung für den Zugang zum Internet ermöglicht. Kabel Modems basieren auf der Infrastruktur des Kabelfernsehens. In anderen Worten kommen die Daten über die gleichen Leitungen wie beim Kabelfernsehen.
Kanal	Ein Pfad oder ein Link über den Informationen zwischen zwei Geräten übermittelt werden.
Kbps	Abkürzung für “kilobits per second“. Datenübertragungsgeschwindigkeit durch ein Modem oder über ein Netzwerk, gemessen als ein Vielfaches von 1000 Bits pro Sekunde.
LAN	Abkürzung für “local area network“. Eine Gruppe von Computern und anderen Geräten verteilt über einen relativ kleinen Bereich (zum Beispiel ein Gebäude) und mit einem Kommunikationsverbindung verbunden. Dies ermöglicht jedem Gerät mit den anderen Geräten im Netzwerk zu interagieren.
Laufwerk	Ein Speicherbereich, der mit einem Dateiverwaltungssystem formatiert ist und einen Laufwerk Buchstaben hat. Der Speicher kann eine Diskette (welche oft mit Laufwerk A bezeichnet wird), eine Festplatte (normalerweise Laufwerk C), eine CD ROM (normalerweise Laufwerk D) oder ein anderer Speichertyp sein. Sie können den Inhalt eines Laufwerks sehen, wenn Sie auf das Laufwerk-Symbol im Windows Explorer oder im Arbeitsplatz klicken. Laufwerk C (auch bekannt als die Festplatte) beinhaltet das Betriebssystem des Computers und die Programme, die auf dem Computer installiert wurden. Hier können auch viele der Dateien und Ordner abgelegt werden, die Sie erstellt haben.

© Internetagentur Schott GmbH, 2010. All rights reserved.

MAC Adresse	Abkürzung für “media access control“ Adresse. Dies ist die Adresse, die für die Kommunikation zwischen Netzwerk Adaptern im gleichen Subnetz verwendet wird. Jeder Netzwerk Adapter wird mit eine eigenen einzigartigen MAC Adresse produziert.
Mapping (abbilden)	Ein Prozess, der es einem Computer ermöglicht mit einer Ressource zu kommunizieren, die auf einem anderen Computer in einem anderen Netzwerk lokalisiert ist. Zum Beispiel wenn Sie auf einen Ordner zugreifen wollen, der auf einem anderen Computer abgelegt ist, können Sie diesen Ordner abbilden, solange der Computer, auf dem der Ordner abgelegt ist, so konfiguriert ist, dass er den Ordner zur gemeinsamen Nutzung freigibt.
Mbps	Abkürzung für “megabits per second“. Eine Einheit zur Messung der Bandbreite. Die Einheit definiert die Geschwindigkeit, mit der Informationen durch ein Netzwerk oder ein Ethernet Kabel übertragen werden können. Ein Megabyte sind ungefähr gleich viel wie acht Megabits.
Modem	Ein Gerät, das Informationen zwischen Computern überträgt und empfängt.
Multicast	Das Übertragen einer einzelnen Nachricht an mehrere Empfänger. Ein einfaches Beispiel für Multicasting ist das Senden von E-Mails an eine Adressliste. Telefon- und Video-Konferenzen verwenden ebenfalls Multicast, benötigen aber robustere Protokolle und Netzwerke.
NAT	Abkürzung für “network address translation“. Der Prozess des Konvertierens von IP-Adressen, die in einem privaten Netzwerk verwendet werden und den Internet IP-Adressen. NAT ermöglicht, dass alle Computer eines Netzwerkes eine IP-Adresse gemeinsam nutzen.
Netz-infrastruktur	Eine Netzwerkkonfiguration, in dem sich wireless Geräte mit einem wireless Access Point (wie zum Beispiel das IAD) verbinden, anstatt direkt mit jedem anderen Gerät.
Netzwerk	Eine Ansammlung von 2 oder mehr Computern, die miteinander verbunden sind. Diese Computer können den Internetzugang, Dokumente, Drucker und anderes Zubehör gemeinsam nutzen.
Netzwerk Name	Der Name einer Gruppe von Computern, die miteinander verbunden sind und ein Netzwerk bilden.
Netzwerk Drucker	Ein Drucker, der nicht direkt mit einem Computer, aber über eine kabellose oder kabelgebundene Verbindung direkt mit dem Netzwerk verbunden ist.
Paket	Eine Informationseinheit, die als ganzes von einem Gerät zu einem anderen übertragen wird.
PAP	Ein Passwort Authentifizierungsprotokoll. Die einfachste Form einer Authentifizierung, bei welcher der Benutzername und das Passwort über das Netzwerk übertragen werden und mit einer Liste mit Name-Passwort-Paaren verglichen wird. Üblicherweise sind die Passwörter in der Liste verschlüsselt. Die grundlegende Authentifizierung beim HTTP Protokoll verwendet RAP.
PC-Karte	Ein Peripheriegerät, das Speicher, Massenspeicher, Modem Fähigkeit oder andere Netzwerk-Dienste zu einem tragbaren Computer hinzufügen.
PCI Karte	Eine Karte, ausgelegt um in einen PCI Expansionsslot einen PCs zu passen. PCI Karten bieten zusätzliche Funktionen. Zum Beispiel Video Adapter und Netzwerk Interface Karten sind zwei Typen von PCI Karten.
Peer-to-Peer Netzwerk	Ein Netzwerk von zwei oder mehr Computern, die ohne zentralen Server mit einander kommunizieren. Dieses Fehlen der Abhängigkeit von einem Server unterscheidet ein Peer-to-Peer Netzwerk von einem Client/Server Netzwerk.
PING	Ein Protokoll, um zu testen, ob ein bestimmter Computer am Internet angeschlossen ist. Dabei wird ein Paket an die IP-Adresse des entsprechenden Computers gesendet und auf eine Antwort gewartet.
Plug and Play	Ein Set von Spezifikationen, die es ermöglichen, dass ein Computer verschiedene Peripheriegeräte wie Monitore, Modems und Drucker automatisch detektiert und konfiguriert.

© Internetagentur Schott GmbH, 2010. All rights reserved.

Port	Eine physikalische Verbindung über die Daten zwischen einem Computer und anderen Geräten (wie Monitor, Modem oder Drucker), einem Netzwerk oder einem anderen Computer übertragen werden. Kann auch ein Software Kanal für die Netzwerk Kommunikation sein.
PPPoE	Abkürzung für “Point-to-Point Protocol over Ethernet“. Eine Spezifikation um Benutzer eines Ethernet-Netzwerkes mit dem Internet zu verbinden, indem eine Breitbandverbindung verwendet wird (üblicherweise über ein DSL Modem).
PPTP	Abkürzung für Point-to-Point Tunneling Protocol. Dies ist eine Technologie, um VPNs zu kreieren. Da das Internet im Wesentlichen ein offenes Netzwerk ist, wird das Point-to-Point Tunneling Protocol (PPTP) verwendet, um zu gewährleisten, dass eine Nachricht von einem VPN Knoten sicher zu einem anderen VPN Knoten übertragen wird. Mit PPTP können sich Benutzer über das Internet in ihr Unternehmensnetzwerk einwählen.
Profil	Ein Computer basierter Datensatz, der die Software Einstellungen und die Informationen zur Identifikation eines Individuums für ein Netzwerk enthält.
Protokoll	Ein Set von Regeln, welche die Computer verwenden, um über das Netzwerk miteinander zu kommunizieren.
RJ-11 Stecker	Ein Anschluss, der verwendet wird, um Telefonleitungen an ein Gerät (z.B. Modem) oder externe Telefonleitungen anzuschliessen. (6 Pins)
RJ-45 Stecker	Ein Anschluss an den Enden jedes Ethernet Kabels, der das Ethernet Kabel mit anderen Geräten und Computern verbindet. (8 Pins)
Server	Ein Computer, der dem Netzwerk-Benutzer gemeinsam benutzte Ressourcen wie Speicherplatz oder Rechenleistung zur Verfügung stellt,
SNTP	Abkürzung für “Simple Network Time Protocol“. Ein Protokoll, das Computer-Clients ermöglicht Ihre Uhren mit einem Zeit-Server über das Internet zu synchronisieren.
SSID	Abkürzung für “Service Set Identifier“, auch bekannt als wireless Netzwerk Name. Eine SSID identifiziert Ihr Netzwerk eindeutig.
Statische IP-Adresse	Eine permanente Internet-Adresse eines Computers (zugewiesen von einem ISP).
Subnetz	Ein eigenes Netzwerk, das Bestandteil eines grösseren Computernetzwerks ist. Subnetze sind mittels Router verbunden und können eine gemeinsam benutzte Netzwerk-Adresse verwenden, um sich mit dem Internet zu verbinden.
Subnetzmaske	Typischerweise repräsentiert ein Subnetz alle Geräte an einem geografischen Ort, in einem Gebäude oder im selben lokalen Netzwerk (LAN). Wenn das Netzwerk einer Organisation in Subnetze eingeteilt ist, ist es möglich mit einer einzelnen gemeinsam benutzen Netzwerk-Adresse zum Internet zu verbinden. Ähnlich in der Form wie eine IP-Adresse und typischerweise von einem ISP zur Verfügung gestellt. Ein Beispiel für eine Subnetzmaske ist der Wert 255.255.0.0.
Switch	Ein zentrales Gerät, das ähnlich funktioniert wie ein Hub: Weiterleiten von Paketen zu den spezifischen Ports anstatt jedes Paket an jeden Port weiterzuleiten (broadcast). Ein Switch ist effizienter, wenn ein grosses Netzwerk verwendet wird.
Switching	Eine Kommunikationsmethode, die temporäre anstatt permanente Verbindungen benutzt, um einen Link aufzubauen, oder Informationen zwischen zwei Parteien zu routen. Paket Switching und Nachrichten Switching ermöglichen irgendwelchen zwei Parteien in einem Computernetzwerk Informationen auszutauschen. Nachrichten werden über Zwischenstationen geroutet (switched). Dies dient zur Verbindung des Senders mit dem Empfänger.

© Internetagentur Schott GmbH, 2010. All rights reserved.

TCP / IP	Abkürzung für “Transmission Control Protocol/Internet Protocol“. Ein Netzwerkprotokoll, das Computern erlaubt über miteinander verbundene Netzwerke und über das Internet zu kommunizieren. Jeder Computer der am Internet angeschlossen ist, kommuniziert über TCP/IP
Treiber	Ein Gerät, dass die Kommunikation vermittelt zwischen dem Computer und dem Netzwerkadapter, der auf diesem Computer installiert ist.
USB	Abkürzung für “universal serial bus“. USB ist ein plug-and-play Schnittstelle zwischen einem Computer und einem Zusatzgerät (wie Audio-Player, Joystick, Tastatur, Telefone, Scanner und Drucker). Mit USB kann ein neues Gerät an Ihrem Computer angeschlossen werden, ohne eine Adapter-Karte anschliessen zu müssen oder sogar den PC neu zu starten.
USB Stecker	Das Endstück eines USB Kabels, das mit einem USB Anschluss verbunden wird. Er ist gut 1cm breit, rechteckig und etwas flach.
USB Anschluss	Der rechteckige Slot in einem Computer, in den ein USB Stecker eingesteckt werden kann.
Vermittlungs-netzwerk	Ein Kommunikationsnetzwerk, das Switches benutzt, um eine Verbindung zwischen Parteien aufzubauen.
Ver-schlüsselung	Die Übersetzung von Daten in einen geheimen Code. Verschlüsselung ist die effektivste Art, um Datensicherheit zu erreichen. Um eine verschlüsselte Datei zu lesen, müssen Sie Zugriff auf den geheimen Schlüssel oder das Passwort haben, welches Ihnen ermöglicht die Datei zu entschlüsseln.
Virtueller Server	Eine von mehreren Web Seiten, die auf dem gleichen Server laufen, jede mit einem eindeutigen Domain Name und einer eindeutigen IP-Adresse.
VPN	Ein Virtual Private Network (VPN) ist ein privates Netzwerk, das Gebrauch macht von der öffentlichen Telekommunikationsinfrastruktur. Der Datenschutz wird durch die Verwendung eines Tunnel-Protokoll und Sicherheitsprozeduren aufrecht erhalten
WAN	Abkürzung für “wide area network“. Ein geografisch ausgedehntes Netzwerk, das viele verbundene lokale Netzwerke enthalten kann.
Wi-Fi	Ein oft benutzter Ausdruck, der den wireless 802.11b Standard beschreibt.
Wireless	Bezieht sich auf eine Technologie, die Computer ohne Kabel miteinander verbindet. Wireless Geräte benutzen Funkübertragung, um Computer in einem Netzwerk miteinander zu verbinden. Funk-Signale können durch Mauern, Decken und Böden übertragen werden, so dass Sie Computer, die in verschiedenen Räumen in einem Haus sind, miteinander verbinden können, ohne sie physikalisch aneinander zu binden.
Wireless Access Point	Ein Gerät, das Daten zwischen wireless Computern oder zwischen wireless Computern und verkabelten Computer in einem Netzwerk austauscht.
Wireless Netzwerkname	Der Name einer Gruppe von Computern, die miteinander verbunden sind und ein Netzwerk bilden.
Wireless Sicherheit	Ein Verschlüsselungsmechanismus für wireless Netzwerk, der hilft die Daten zu schützen, die über das wireless Netzwerk übertragen werden.
WLAN	Abkürzung für “wireless local area network“. Ein Netzwerk, das nur auf wireless Technologien beruht, um die Geräte miteinander zu verbinden.
VLAN	Abkürzung für “virtual local area network“. Eine Technologie, die es erlaubt ein physikalisches Netzwerk in verschiedene Netzwerke zu unterteilen, wobei die einzelnen Netzwerke keinen Zugriff auf die anderen haben.

© Internetagentur Schott GmbH, 2010. All rights reserved.

10.1Tabelle mit Abkürzungen

ALG	Application-Level Gateway
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CNG	Comfort Noise Generation
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DND	Do not Disturb
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EC	Echo Cancellation
ESSID	Extended Service Set Identifier
ETH	Ethernet
EWAN	Ethernet WAN
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyper Text Transport Protocol
HTTPS	HTTP Secure
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
IPoE	Internet Protocol over Ethernet
IPP	Internet Printing Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MPoA	Multiprotocol Encapsulation over ATM
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OAM	Operations and Maintenance
PBC	Push Button Configuration
PDA	Personal Digital Assistant
PIN	Personal Identification Number
POP3	Post Office Protocol 3
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
PSK	Pre-Shared Key

© Internetagentur Schott GmbH, 2010. All rights reserved.

PSTN	Public Switched Telephone Network
PTM	Packet Transfer Mode
QoS	Quality of Service
RFC	Request for Comment
RIP	Routing Information Protocol
RTP	Real-Time Transport Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple NTP
SPI	Stateful Packet Inspection
SRA	Seamless Rate Adoption
SSH	Secure Shell
SSID	Service Set Identifier
STB	Set-Top-Box
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URL	Universal Resource Locator
USB	Universal Serial Bus
VAD	Voice Activity Detection
VCI	Virtual Channel Identifier
VLAN	Virtual LAN
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VoIP	Voice over IP
WAN	Wide Area Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WoL	Wake on LAN
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

© Internetagentur Schott GmbH, 2010. All rights reserved.

11. CE-Konformitätserklärung

Das Gerät erfüllt die folgenden EU-Richtlinien:

1999/5/EC	Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität (R&TTE)
2004/108/EC	Elektromagnetische Verträglichkeit (EMC)
2006/95/EC	Niederspannungs-Richtlinie (LVD)
1999/519/EC	Exposition der Bevölkerung gegenüber EMF
2005/32/EC	Umweltgerechte Gestaltung energiebetriebener Produkte (EuP)
2002/95/EC	Beschränkung bestimmter gefährlicher Stoffe (RoHS)

Die kompletten Testberichte können unter folgender Adresse bezogen werden:
Internetagentur Schott GmbH
Cent-Hoheneichstr. 11
D-96191 Viereth-Trunstadt
Deutschland

Länderhinweis:
Die Funktechnik dieses Gerätes ist für die Verwendung in allen Ländern der Europäischen Union sowie in der Schweiz, in Norwegen und Island vorgesehen. In Frankreich ist nur der Betrieb in geschlossenen Räumen zulässig.

Internetagentur Schott GmbH
Cent-Hoheneichstr. 11
D-96191 Viereth-Trunstadt
Tel. +49 9503 8099999 (DE)
Tel. +49 9503 8099998 (EN)
Fax.+49 9503 50440690
www.satspeed.com

© Internetagentur Schott GmbH, 2010. All rights reserved.